Sorbonne Université

Ecole Doctorale

Doctorat, Communication Systems Department

ARCHITECTURE FOR SIMULTANEOUS MULTI-STANDARD SOFTWARE DEFINED RADIO RECEIVER

SUMIT KUMAR

Thèse dirigée par Prof. Florian Kaltenberger, Eurecom, France

Présentée et soutenue publiquement le 12 April 2019

Devant un jury composé de

Priv.-Doz. DI Dr. techn. Thomas Zemen	Rapporteur
Prof. Ghaya REKAYA-BEN OTHMAN	Rapporteur
Prof. Michel Terre	Jury
Prof. Jérôme Häerri	Jury
Prof. Leonardo Cardoso	Jury
Prof. George C. Alexandropoulos	Jury

Acknowledgements

Foremost, I would like to express my sincere gratitude to my supervisor Prof. Florian Kaltenberger for the continuous support of my Ph.D. studies and related research, for his patience, motivation, flexibility, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. His ability to direct me towards alternative solutions when all the intuitive paths were blocked was precious. I could not have imagined having a better advisor and mentor for my Ph.D. study.

I would also like to sincerely thank my co-advisors from Siemens AG Corporate Technology, Munich, Dr. Alejandro Ramirez, and Dr. Bernhard Kloiber for their insightful critical comments which helped me improve my practical understanding of the subject matter.

I am deeply grateful to Kalyana Gopala, Elena Lukashova and Cedric Roux for their encouraging and stimulating discussions on the subject matter as well as day-to-day life matters.

Besides, I am very thankful to my friends Pramod Bacchav, Tsu Han Wangts, Roya Gholamipour, Harald Bayerlin, Rajeev Gangula, Konstantinos Alexandris, Christo Thomas and Leela Guddupudi for providing the happy distraction to rest my mind outside of my research.

Last but not least, I am thankful to my family members for their continuous support, encouragement and sympathetic ear during my Ph.D.

Contents

Abstract **9**

1 Introduction **12**
1.1 What is a Software Defined Radio? . . . 12
1.2 Motivation and Problem Statement: Simultaneous Multi-Standard SDR . . . 13
1.3 Organization of the thesis . . . 15
1.4 Published Articles . . . 16
1.5 Submitted Articles . . . 16
1.6 Demonstrations . . . 16

2 Simultaneous Multi-Standard Software Defined Radio **17**
2.1 SMS-SDR . . . 17
2.2 Challenges in Implementing SMS-SDR . . . 18
2.2.1 Finite ADC bit width . . . 19
2.2.2 Channelization . . . 20
2.2.3 Cross Technology Co-Channel Interference . . . 21
2.3 Our Approach to Implement SMS-SDR . . . 21

3 Related Work and State of the Art **24**
3.1 Co-Channel Interference . . . 24
3.2 Collision Avoidance . . . 25
3.3 Interference Cancellation . . . 27
3.4 Directional Antennas . . . 27
3.5 Interference Nulling . . . 28
3.6 Multi-Standard Software Defined Radio . . . 30
3.7 Summary . . . 31

4 CT-CCI Mitigation Between Wideband OFDM and Narrowband Signals **32**
4.1 Physical Layer of IEEE 802.11g and ZigBee . . . 32
4.1.3 Interference Scenarios . . . 34
4.2 Mitigating CCI in Single Antenna IEEE 802.11g Receiver Caused by ZigBee . . . 37
4.2.2 Log-Likelihood Ratio Scaling with Localized Noise Variance of Interfered IEEE 802.11g Subcarriers (LNV-SC) . . . 38
4.2.4 Multiple Narrowband Interference Detection . . . 40
4.2.5 Simulations and Results . . . 41
4.2.6 Discussion . . . 43
4.2.8 Successive Interference Cancellation of ZigBee from IEEE 802.11g . . . 44
4.2.10 Simulations and Results . . . 46
4.2.11 Discussion . . . 46
4.3 Testing LNV-SC for its General Applicability . . . 48
4.4.3 Mitigating CCI in Single-antenna IEEE 802.11ax Receiver Caused by SC-FDMA . . . 49
4.4.4 Applying LNV-SC to IEEE 802.11ax . . . 50
4.4.5 Simulations and Results . . . 50
4.4.6 Discussion . . . 51
4.5 Mitigating CCI in Multi-antenna IEEE 802.11g Receiver Caused by ZigBee . . . 51
4.5.4 Maximum Ratio Combiner with Log-Likelihood Ratio Scaling (MLSC) . . . 54
4.5.5 Diversity Combiner TIMO (DC-TIMO) . . . 55

4.5.6 Simulations and Results . . . 55
4.5.7 Discussion . . . 57
4.6 Mitigating CCI in Single Antenna ZigBee receiver caused by IEEE 802.11g . . . 58
4.6.1 Successive Interference Cancellation of IEEE 802.11g from ZigBee . . . 58
4.6.2 Simulations and Results . . . 59
4.6.3 Discussion . . . 61
4.7 Mitigating CCI in Multi-Antenna ZigBee receiver caused by IEEE 802.11g . . . 61
4.7.1 SIC of IEEE 802.11g followed by MRC of ZigBee . . . 61
4.7.2 Simulations and Results . . . 61
4.7.3 Discussions . . . 63
4.8 Summary of the Methods . . . 63
4.9 Publications . . . 65

5 CT-CCI Mitigation Between Two OFDM Signals 66
5.1 Physical Layer of IEEE 802.11ac and LTE-LAA . . . 66
5.1.3 Interference Scenarios . . . 69
5.2 Mitigating CCI in Single Antenna IEEE 802.11ac Receiver Caused by LTE-LAA . . . 70
5.2.1 SIC of LTE-LAA CCI from IEEE 802.11ac . . . 70
5.2.2 SIC of LTE-LAA CCI from IEEE 802.11ac under Slow Fading Channel (Indoor Environment) . . . 71
5.2.3 Simulations and Results . . . 74
5.2.4 Discussion . . . 79
5.3 Mitigating Interference in Multi-Antenna IEEE 802.11ac Receiver Caused by LTE-LAA . . . 79
5.3.1 SIC of LTE-LAA from IEEE 802.11ac followed by MRC . . . 79
5.3.2 Simulations and Results . . . 79
5.3.3 Discussion . . . 81
5.4 Summary of the Methods . . . 81
5.5 Publications . . . 83

6 Simultaneously Decoding Heterogeneous Signals 84
6.1 Decision Tree: Interference Detection . . . 84
6.1.1 Interference Detection . . . 87
6.2 Decision Tree: Interference Mitigation . . . 87
6.2.1 Single Antenna Receiver . . . 88
6.2.2 Multi-Antenna Receiver . . . 89
6.3 Discussion . . . 92

7 SDR Implementations 94
7.1 SDR Hardware and Software Tools . . . 94
7.2 LNV-SC . . . 96
7.3 SBMRC . . . 96
7.4 OTA Testing: Test Set-Up, Experiments, and Results . . . 97
7.5 ZigBee Double Receiver . . . 103
7.6 Filter Bank Channelizer . . . 104
7.7 Demonstrations . . . 107

8 Conclusions and Future Research 108
8.1 Conclusions . . . 108
8.2 Future Work . . . 109

A 110
A.1 Round Trip and Receive Latency Measurement in USRP . . . 110

B 116
B.1 Soft Bit Metrics . . . 116
B.2 Soft Bit Maximal Ratio Combiner (SBMRC) . . . 117
B.3 Computation of Log Likelihood Ratio . . . 119

Bibliography 120

List of Figures

1.1 Block diagram of a typical Software Defined Radio . . . 12
1.2 WiFi Bluetooth Co-existence in a System on Chip (SOC). W_1 and B_1 are monolithic WiFi and Bluetooth chips respectively on a single device. While W_2 and B_2 are WiFi and Bluetooth chips on separate devices. . . . 14

2.1 A plausible schematic of a Simultaneous Multi-Standard SDR (SMS-SDR) . . . 17
2.2 Due to finite ADC bitwidth/resolution, the weaker signal cannot span through the entire dynamic range of the ADC in the presence of a stronger signal. This results in noise like representation of the weaker signal after digitization. . . . 19
2.3 Frequency domain overlap of signals during CCI . . . 20
2.4 (a) Direct Conversion Receiver (b) Intermediate Frequency Receiver . . . 20
2.5 Example flow diagram for mitigating CT-CCI from two heterogeneous wireless standards operating on overlapped frequency bands . . . 23

3.1 A typical proceedure of CSMA/CA . . . 25
3.2 Hidden and Blind terminal scenarios between IEEE 802.11g and ZigBee . . . 26
3.3 Radiation pattern of omni directional and directional antennas . . . 28
3.4 Constructive and destructive addition of same signal coming from different paths . . . 29
3.5 Method for multi-standard software defined radio base-band processing [65] . . . 30

4.1 IEEE 802.11g Subcarrier Allocation . . . 33
4.2 IEEE 802.11g Non-HT frame format . . . 33
4.3 ZigBee OSI Architecture . . . 34
4.4 ZigBee Frame Format . . . 34
4.5 Frequency Allocation of IEEE 802.11g in 2.4 GHz band . . . 35
4.6 Frequency Allocation of ZigBee in 2.4 GHz band . . . 35
4.7 IEEE 802.11g and ZigBee overlap . . . 35
4.8 PER of single antenna WiFi receiver in the presence and absence of single antenna ZigBee transmitter(transmit power -85 dBm). For all IEEE 802.11g MCS, we observe severe PER degradation. . . . 36
4.9 PER of single antenna ZigBee receiver in the presence and absence of single antenna IEEE 802.11g transmitter(transmit power -85 dBm). Even at -85 dBm, which is lower than the minimum receiver sensitivity of IEEE 802.11g, ZigBee observes severe PER degradation. . . . 36
4.10 Set of interfered and interference-free WiFi Subcarriers facing interference by 4 Co-Channel ZigBee Interferers . . . 39
4.11 LNV estimates corresponding to 4 ZigBee Interferers. Distinguish lobes appear at ZigBee center frequencies due to LNV estimation. . . . 39
4.12 Flow Chart of Interference Detection and LLR Scaling. LLR scaling using LNV (LNV-SC) to be performed only during interference. . . . 40
4.13 Performance of LNV-SC for IEEE 802.11g MCS 0 and 2 facing interference from single ZigBee channel at -85 dBm. LNV-SC observes an average transmit power gain of 3.7 dB over Conv-SC for all the MCS. . . . 42
4.14 Performance of LNV-SC for IEEE 802.11g MCS 0 and 2 facing interference from two ZigBee channels at -85 dBm. LNV-SC observes an average transmit power gain of 3 dB over Conv-SC for all the MCS. . . . 42
4.15 Performance of LNV-SC for IEEE 802.11g MCS 0 and 2 facing interference from four ZigBee channels at -85 dBm. LNV-SC observes an average transmit power gain of 1.5 dB over Conv-SC for all the MCS. . . . 43

4.16 Noise Level Ratio: Ratio of the LNV of the interfered region to that of the region without interference for fixed WiFi TXP -80 dBm. Even at low interference TxP of -100 dBm, the NLR is 6.5 dB which is sufficient to detect the presence of interference. 43
4.17 Synchronization Error Rate (SER) of IEEE 802.11g MCS 2 and 4 after SIC of ZigBee (−80 dBm). SER for both MCS is similar as the preamble of IEEE 802.11g is BPSK mobulated regardless of the MCS 47
4.18 Packet Error Rate of IEEE 802.11g, MCS 2 after SIC of ZigBee (−80 dBm). Region over which SIC provides gain is highlighted in green rectangle. 47
4.19 Packet Error Rate of IEEE 802.11g, MCS 4 after SIC of ZigBee (−80 dBm). Region over which SIC provides gain is highlighted in green rectangle. 47
4.20 Single user frame format of IEEE 802.11ax 49
4.21 A block diagram of SC-FDMA 49
4.22 Comparison of LNV-SC and Conv-SC in improving PER of IEEE 802.11ax MCS 0 facing interference from 3 MHz SC-FDMA (−85 dBm) signal. LNV-SC performs better than Conv-SC 51
4.23 Comparison of LNV-SC and Conv-SC in improving PER of IEEE 802.11ax MCS 0 facing interference from 5 MHz SC-FDMA (−85 dBm) signal. LNV-SC performs better than Conv-SC 51
4.24 Signal Model: Single Antenna IEEE 802.11g Transmitter, Single Antenna ZigBee Interferer and Two Antenna IEEE 802.11g receiver 52
4.25 Schematic of Proposed MLSC for 2 Antenna WiFi Receiver 55
4.26 Comparison of MRC (with Conv-SC), OC and MLSC, for IEEE 802.11g MCS 0 and ZigBee TxP -85 dBm 56
4.27 Comparison of MRC(with Conv-SC), MLSC and TIMO for IEEE 802.11g MCS 0. MLSC performs better than both MRC (with Conv-SC) and TIMO. ZigBee TxP −85 dBm 57
4.28 Comparison of MRC(with Conv-SC), MLSC and TIMO for IEEE 802.11g MCS 2. MLSC performs better than both MRC (with Conv-SC) and TIMO. ZigBee TxP −85 dBm 57
4.29 Comparison of TIMO and DC-TIMO for IEEE 802.11g MCS 0. DC-TIMO benefits from the additional diversity gains. ZigBee TxP −85 dBm 58
4.30 PER of ZigBee after SIC of single channel IEEE 802.11g(MCS 0, TxP −85 dBm). 60
4.31 PER of ZigBee after SIC of single channel IEEE 802.11g (MCS 2, TxP −85 dBm). 60
4.32 Schematic of SIC-MRC Receiver when IEEE 802.11g is the stronger signal and ZigBee is the weaker signal 62
4.33 PER comparison of ZigBee when SIC, SIC-MRC and Only MRC is applied, at IEEE 802.11g MCS 0, TxP −85 dBm. SIC-MRC performs better than SIC. Plain MRC is also capable of reducing PER in the event of interference. 62
4.34 PER comparison of ZigBee when SIC, SIC-MRC and Only MRC is applied, at IEEE 802.11g MCS 2, TxP −85 dBm. SIC-MRC performs better than SIC. Plain MRC is also capable of reducing PER in the event of interference. 62

5.1 Frequency Allocation of IEEE 802.11ac in 5 GHz band (FCC, North America) 67
5.2 IEEE 802.11 VHT Frame Format 67
5.3 IEEE 802.11ac subcarrier allocation 68
5.4 LTE-LAA Downlink Resource Grid 69
5.5 Time Domain LTE-LAA 69
5.6 An indoor deployment scenario of single antenna WiFi Tx (W), single antenna LTE-LAA Tx (L) and single antenna WiFi Plus LTE-LAA dual technology receiver (RX) 72
5.7 Proposed Scheme to Capture LTE-LAA Channel in the past and apply them in future. 72
5.8 Synchronization error of IEEE 802.11ac MCS 0: With and Without SIC, LTE-LAA −80 dBm. Plot indicates that with SIC, the lost packets of IEEE 802.11ac caused by collision can be recovered. 75
5.9 Frame Error for IEEE 802.11ac MCS 0: With and Without Using SIC, LTE-LAA TxP −80 dBm 76
5.10 Frame Error for IEEE 802.11ac MCS 2: With and Without Using SIC, LTE-LAA TxP −80 dBm 76
5.11 Frame Error for IEEE 802.11ac MCS 4: With and Without Using SIC, LTE-LAA TxP −80 dBm 76
5.12 Synchronization error of IEEE 802.11ac MCS 0 at inter frame arrival times 2 ms, 10 ms and 20 ms, LTE-LAA −80 dBm 77
5.13 Frame Error for IEEE 802.11ac MCS 0 at inter frame arrival times 2ms, 10ms and 20ms, LTE-LAA −80 dBm 78

5.14 Frame Error for IEEE 802.11ac MCS 2 at inter frame arrival times 2ms, 10ms and 20ms, LTE-LAA −80 dBm . . . 78
5.15 Frame Error for IEEE 802.11ac MCS 4 at inter frame arrival times 2ms, 10ms and 20ms, LTE-LAA −80 dBm . . . 78
5.16 Frame error for IEEE 802.11ac MCS 0: Performing SBMRC after SIC in a dual antenna receiver, LTE-LAA −80 dBm . . . 80
5.17 Frame error for IEEE 802.11ac MCS 2: Performing SBMRC after SIC in a dual antenna receiver, LTE-LAA −80 dBm . . . 80
5.18 Frame error for IEEE 802.11ac MCS 4: Performing SBMRC after SIC in a dual antenna receiver, LTE-LAA −80 dBm . . . 80

6.1 Decision tree for the parallel receivers attempting to decode signals $S1$ and $S2$ simultaneously. The result after parsing the decision trees is either decoding the signals or detecting the interference. The figure continues to Fig. 6.2 . . . 85
6.2 Continuation of Fig. 6.1 . . . 85
6.3 Noise Level Ratio based interference detection in OFDM systems. Wideband OFDM can detect narrowband interference in case the interferer is narrowband as in (a) or there is a partial overlap as in (c). However it fails when both signals have comparable bandwidths as in (b) . . . 88
6.4 (a) Decision tree to mitigate CT-CCI and recover wideband OFDM signal (b) Decision tree to mitigate CT-CCI and recover narrowband signal . . . 90
6.5 (a) Decision tree to mitigate CT-CCI and recover OFDM signal in case of interference with another OFDM signal (b) Decision tree to mitigate CT-CCI and recover Non-OFDM signal in case of interference with another Non-OFDM signal . . . 90
6.6 (a) Decision tree to mitigate CT-CCI and recover wideband OFDM signal(b) Decision tree to mitigate CT-CCI and recover narrowband signal . . . 91
6.7 (a) Decision tree to mitigate CT-CCI and recover OFDM signal facing interference from another OFDM signal (b) Decision tree to mitigate CT-CCI and recover a non-OFDM signal facing interference from another non-OFDM signal . . . 91

7.1 Soft Bit Maximal Ratio Combiner with LLR Scaling . . . 97
7.2 Over-the-air test set-Up: USRP B210, RF Cage and General Purpose CPU . . . 98
7.3 Over-the-air Test Schematic corresponding to Section 7.4 . . . 98
7.4 LNV-SC (proposed method) in the single interferer case leads to more IEEE 802.11g frames passing CRC test compared to Conv-SC (conventional method) at a lower IEEE 802.11g TXP. This is observed for both the experimented interferer TXP . . . 100
7.5 LNV-SC (proposed method) in the two interferer case also leads to more IEEE 802.11g frames passing CRC test compared to Conv-SC (conventional method) at a lower IEEE 802.11g TXP. This is observed for both the experimented interferer TXP . . . 101
7.6 Branch-2 is partially covered with aluminum foil thus, receives lesser packets than Branch-1. In this case, SB-MLSC tracks Branch-1 which receives more packet than Branch-2. . . . 101
7.7 Branch-1 is fully covered with aluminum foil and hence ceases to receive any packet. In this case, SB-MLSC tracks Branch-2 when Branch-1 is killed. . . . 102
7.8 Scrambled aluminum foils are placed inside RF cage resulting in multi-apth reflections. In this case, SB-MLSC provides diversity gain, i.e., receives more packet than both Branch-1 and Branch-2. . . . 102
7.9 GNU Radio Schematic For Double Receiver. The receiver is tuned to ZigBee channel-16 in 2.4GHz ISM band. A double receiver operates by decoding all the branches simultaneously. This is contrast to selection combiner which selects one out of many available branches. . . . 103
7.10 Performance of ZigBee double receiver under several normalized receiver gain. As the gain increases, both the antenna branches show similar performance. The experiment shows that diversity based reception show better performance when the system operate at the boundary of noise limited region. . . . 105
7.11 Functionality of a basic spectrum carving module for SMS-SDR. We have used spectrum carving and channelizing synonymously in this thesis. . . . 106
7.12 GUI of GNU Radio FreqXlating Filter Options. The block can be configured to perform frequency translation and decimation (if required) simultaneously. . . . 106

A.1 Round trip latency test setup for USRP B210 and USRP X300 . . . 111
A.2 Receive latency test setup for USRP B210 and USRP X300 . . . 113
A.3 Hardware Setup . . . 113

A.4 Manual view of receive latency on Oscilloscope 113
A.5 Components contributing to receive latency 114
A.6 Receive Latency for B210 114
A.7 Receive Latency for X300 114

B.1 Soft bit metrics calculation in QPSK 117
B.2 MRC vs SBMRC in the absence of interference. Both of them perform the same in the absence of interference under the same channel conditions. 118

List of Tables

1.1 Notable SDR Implementation of Wireless Standards using SDR 13

3.1 Relative Comparison of CCI and CT-CCI Mitigation Techniques 31

4.1 Simulation Parameters 41
4.2 Transmit Power Gain(dB) of LNV-SC compared to Conv-SC 41
4.3 SC-FDMA specifications used in LTE Uplink (20 MHz) 49
4.4 Simulation parameters for interference between IEEE 802.11ax and SC-FDMA 50
4.5 Methods to detect interference 63
4.6 Methods to Mitigate CT-CCI between wideband OFDM and narrowband signals 64

5.1 Simulation Parameters for LTE-LAA and IEEE 802.11ac Experiments 74
5.2 Methods to Mitigate CT-CCI between two wideband OFDM signals 82

7.1 List of surveyed SDR Hardware Platforms 95
7.2 List of Hardware for OTA tests of LNV-SC, SBMRC and SB-MLSC 97
7.3 Hardware used for OTA Tests of ZigBee Double Receiver 104

A.1 UHD stream args used for latency_test.cpp 111
A.2 UHD Params used for Receive Latency Test 112
A.3 Receive latency test results 113

Abstract

In the past, there have been several works on reconfiguring a Software Defined Radio (SDR) to realize multiple wireless standards; however, no attempts have been made to decode information from multiple heterogeneous wireless standards *simultaneously*. Motivated by the capabilities of SDR, in this work, we theorize a Simultaneous Multi-Standard Software Defined Radio (SMS-SDR) receiver. An SMS-SDR receiver will be capable of decoding information from multiple heterogeneous wireless standards "simultaneously" using a single RF front-end. Besides, the SMS-SDR will be developed using Commercial-off-the-shelf (COTS) SDR hardware. Our target networks are random access networks such as IEEE 802.11g, IEEE 802.11ac, IEEE 802.11ax, LTE-LAA, IEEE 802.15.4 operating in unlicensed 2.4 and 5 GHz bands. In the unlicensed bands, these standards operate without any centralized coordination and face severe Cross technology Co-Channel Interference (CT-CCI) as their frequency bands of operation overlaps. Our approach towards implementing SMS-SDR is to recover multiple heterogeneous signals which have interfered with each other. We develop several novel baseband signal processing algorithms to mitigate the CCI in single and multi-antenna receivers. Among many other, we identified CT-CCI as one of the significant challenges to realize an SMS-SDR receiver and develop several novel methods to mitigate CT-CCI for single and multi-antenna systems. In addition, we improved several state-of-the-art methods of interference mitigation. We chose the use case of narrowband and wideband signals with particular attention to OFDM based systems as OFDM has been a key physical layer technique of modern wireless standards such as IEEE 802.11 family and 4G. While the development, we focus on the methods which can operate at the receiver in a standalone fashion, i.e., without any cooperation from the transmitter or the base station. In this way, they are suitable for random access networks operating in the license-free bands. Besides, the algorithms can be integrated into the existing infrastructure without any significant effort. Finally, our interference mitigating methods are used to develop decision trees which recommend the sequence of steps to be performed in order to mitigate the interference between any two heterogeneous signals. The next phase of our work is dedicated to the validation of the interference mitigation schemes and their real-world applicability. For that, we implemented some of our selected algorithms on General Purpose Processor (GPP) based SDR using software packages such as GNU Radio and Openairinterface and COTS hardware Ettus USRP. Next we, performed over-the-air (OTA) testing of our interference mitigating receiver against standard-compliant waveforms under a controlled environment inside a Faraday cage. The results of our OTA tests fall in close agreement with our simulation results showing the real-world applicability of our interference mitigating methods. Our works have significant potential

for application and expansion in the upcoming 5G networks, where problems arising due to interference have been foreseen. Two of such examples are Co-existence between Ultra Reliable Low Latency Communication (URLLC), Massive Machine Type Communication (mMTC) and Enhanced Mobile Broadband. Among many other solutions, Non-orthogonal Multiple Access (NOMA) based methods are being researched. The other one is Ultra Dense Networks (UDN) where the dense and random deployment of heterogeneous network infrastructures results in unpredictable interference scenarios compared to current sparse networks.

Acronyms

AWGN	Additive White Gaussian Noise
CCI	Co-Channel Interefrence
CT-CCI	Cross Technology Co-Channel Interefrence
FPGA	Field Programmable Gate Array
GPP	General Purpose Processor
LNV	Localized Noise Variances
LNV-Sc	Localized Noise Variance based Log Likelihood Ratio Scaling of OFDM subcarriers
MRC	Maximal Ratio Combining
MIMO	Multiple Input Multiple Output
MLSC	Maximal Ratio Combining and Log Likelihood Ratio Scaling of OFDM subcarriers
OC	Optimal Combiner
OFDM	Orthogonal Frequency Division Multiplexing
OTA	Over-the-air
RF	Radio Frequency
SNR	Signal-to-Noise Ratio
SDR	Software Defined Radio
SMS-SDR	Simultaneous Multi-Standard Software Defined Radio
SBMRC	Soft Bit Maximal Ratio Combining
SIC	Successive Interference Cancellation
TIMO	Tecgnology Independent MIMO
USRP	Universal Software Radio Peripheral
URLLC	Ultra Reliable Low Latency Communication
UDN	Ultra Dense Networks

Chapter 1

Introduction

This chapter provides a brief introduction to the Software Defined Radio (SDR). Difference between various SDR concepts have been explained, and the motivation for Simultaneous Multi-Standard Software Defined Radio (SMS-SDR) has been developed. Details of the related publications and demonstrations performed during the Ph.D. work is also provided along with the organization of the thesis.

1.1 What is a Software Defined Radio?

An Software Defined Radio (SDR) uses programmable hardware such as Digital Signal Processor (DSP) and Field Programmable Gate Array (FPGA) for performing the necessary signal processing tasks in the transceiver [75],[92]. DSP and FPGA enable an SDR to define and control the functionalities of the transceiver just by manipulating the software. The programmability using software offers greater flexibility and longer product life compared to Hardware Defined Radio (HDR) which has little or no software control and is designed to be discarded and replaced. Fig. 1.1 shows the block diagram of a typical SDR transceiver. It has two main components: configurable RF front-end (orange block) and programmable back-end (blue block). For the receive chain (Rx), the RF front-end of SDR mainly consists of Low Noise Amplifier (LNA)[1], Analog to Digital Convertor (ADC)[2], Filters, Mixers etc. All the RF front-end components are configurable through software commands via the control bus. Examples of software configurable RF front-end include Universal Software Radio Peripehral (USRP) Daughter Boards provided by Ettus Research [4] which are configurable over either

[1]Power Amplifier (PA) for the Transmit chain Tx
[2]Digital to Analog Convertor (DAC) for the Tx

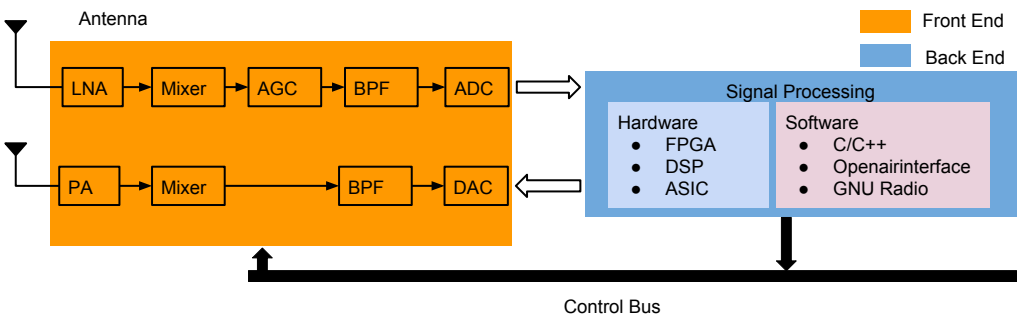


Fig. 1.1. Block diagram of a typical Software Defined Radio

USB or PCI ports. The programmable back-end is the heart of any SDR which is responsible for all the signal processing tasks. There are two different methods in which the programmable back-end is implemented. They are called *FPGA based SDR*, and *General Purpose Processor (GPP) based SDR*. An FPGA based SDR performs the majority of the signal processing tasks inside the FPGA with minimal support form the GPP. FPGA based SDRs are preferred in time-critical signal processing tasks as the vicinity of the RF front-end to the FPGA reduces the interconnection delay caused by USB or PCI ports, for example, [7][11][3] . GPP based SDRs allocate the computationally intensive signal processing tasks to the FPGA and perform lesser intensive tasks using the GPP, for example, [10] [8]. On the software side, to program the hardware of SDR, a majority of the developers use C, C++, and Python for GPP based SDR while VHDL and Verilog for FPGA based SDR. Based on these programming languages, several software packages have evolved such as Openairinterface [50], GNU Radio [6], Microsoft SORA [89], MATLAB [5], and LabView [9]. Due to the flexibility in programming and affordable prices, both GPP and FPGA based SDRs have become popular in academia and industry for quick prototyping of research related to wireless communication standards. Some of the notable implementations of wireless standards using SDRs are tabulated in Table 1.1

Table 1.1: Notable SDR Implementation of Wireless Standards using SDR

Wireless Standard	**SDR Hardware**	**SDR Software**	**SDR Type**
IEEE 802.11a/g/p	USRP [25]	GNU Radio	GPP
IEEE 802.15.4	USRP [24]	GNU Radio	GPP
IEEE 802.11a	USRP [7]	LabView	FPGA
LTE, LTE-A	USRP, Blade RF, Lime SDR [1]	Openairinterface	GPP
IEEE 802.11a/b/g	SORA [8]	Microsoft SORA SDK	FPGA

1.2 Motivation and Problem Statement: Simultaneous Multi-Standard SDR

Due to its ease of reconfigurability, an SDR based system is preferred for cellular base station deployments in 3G/4G/5G communication systems [61][38]. Still, SDR technology is too costly to use in commercial smartphones and consumer electronic devices. Nonetheless, there have been some recent attempts of developing SDR based modems such as NVIDIA © i500 LTE modem [66]. With such modems, the current focus is towards reconfigurability which will allow for rapid development and deployment of future-proof designs. For example, the NVIDIA i500 will first ship with LTE Category 3 support; it will be upgraded via software to support LTE Category 4 with Carrier Aggregation.

In the current high-end smartphones and tablets, support for multiple standards in the single device has become a de facto [75][65] practice. For example IEEE 802.11(a/b/g/n/ac): popularly known as WiFi, IEEE 802.15.1: known as Bluetooth, IEEE 802.15 WPAN: known as RFID, Near Field Communication (NFC), GPS, etc.

Let's take the example of WiFi and Bluetooth operating in 2.4 GHz band. Currently, both the standards are integrated monolithically on a single chip and share the antenna to save cost and space,

[3]Before the advent of FPGA, DSP (Digital Signal Processor) based SDR were used. DSPs are advantageous in terms of development infrastructure and developer familiarity. However, as the cost of FPGA has declined, a heterogeneous combination of DSP and FPGA is frequently used.

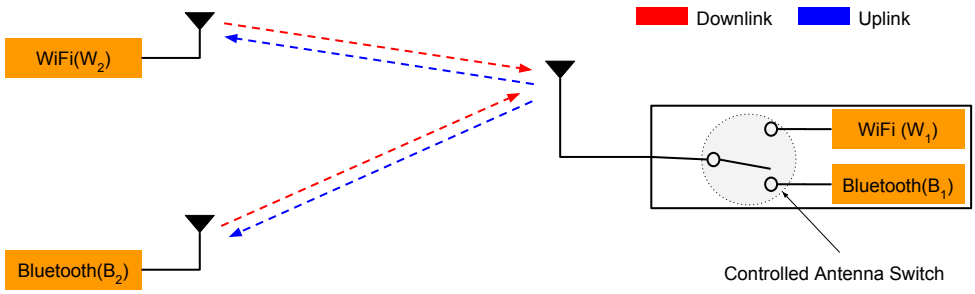


Fig. 1.2. WiFi Bluetooth Co-existence in a System on Chip (SOC). W_1 and B_1 are monolithic WiFi and Bluetooth chips respectively on a single device. While W_2 and B_2 are WiFi and Bluetooth chips on separate devices.

for example, Broadcom BCM43012[2], Cypress CYW43012[3]. Tasks in smartphone or tablets where WiFi and Bluetooth are simultaneously active such as using Bluetooth headset during voice calling over WiFi are very common and it 'appears' that both WiFi and Bluetooth are transmitting/receiving simultaneously; however they don't, since they run in the same frequency band. Wifi transmits using a contention-based mechanism CSMA/CA where before transmission it senses the medium and transmits only if the medium is idle. On the other hand, Bluetooth performs frequency hopping where it transmits briefly on a small chunk of spectrum, then instantly hops to a different frequency to continue the transmission. Chip manufacturers design the transceivers using antenna control switch in such a way that during transmissions only one of them; either WiFi or Bluetooth is active as shown in Fig. 1.2. However, during the downlink traffic, especially during the initial stages of connection, W_2 is unaware of the traffic between B_1 and B_2 as there is no co-ordination between[4] W_2 and B_2, leading to collision, also known as Co-channel Interference (CCI). CCI is a known problem in wireless communication caused by the hidden terminal and blind terminal [82][91].

But, what happens with the frames of WiFi and Bluetooth after they have interfered with each other? If the Signal to Interference Plus Noise Ratio (SINR) is sufficient for both the signals after interference, they can still be detected and decoded; if not, they are simply discarded. Thus, such interference reduces the system throughput because of retransmissions. Several approaches have been researched to address CCI mitigation, and most of them are based on isolation; temporal[5] or frequency[6]. However, any such isolation limits the system throughput again by putting a limitation on the resources. Moreover, isolation based approaches require coordination between transmitters of heterogeneous wireless standards which is not possible without modifying the standard. On the other hand, if the SoC is capable of recovering the lost frame or correct the damaged frame after it is detected, the throughput can be increased for both the involved signals. Besides, such a solution will let both the wireless standards to transmit simultaneously without any contention for the channel.

In this thesis, we attempt to address the problem of CCI between heterogeneous wireless standards operating in shared frequency bands, for example, IEEE 802.11g and IEEE 802.15.4 in the 2.4 GHz ISM band, IEEE 802.11ac and LTE-LAA downlink in the 5 GHz ISM band, IEEE 802.11ax and LTE-LAA(SC-FDMA) in the 5 GHz ISM band. ISM bands are characterized by a license-free operation; hence, all the mentioned standards contend to use the channel without any centralized coordination leading to frequent interference and throughput loss. Summary of the contributions in this thesis is as follows:

[4]Same applies for the downlink transmission between B_2 and B_1 and the ongoing WiFi link
[5]Assignment of different time slots for WiFi and Bluetooth
[6]Assignment of different frequency bands to WiFi and Bluetooth

- Develop new physical layer signal processing methods to mitigate CCI as well as improvise existing CCI mitigation methods which can detect and decode the heterogeneous signals which are lost due to CCI. The signal processing methods will operate standalone on the receivers without the requirement of any coordination from the transmitters.

- Test the developed methods for their applicability in general use cases by doing minimal customizations. For example, wideband and narrowband signals, wideband and wideband signals, etc.

- Develop Software Defined Radio (SDR) prototype for selected methods and verify the agreement between simulations and results form over the air experiments. An SDR prototype enables rapid deployment and customization of CCI methods for new use cases.

With the above contributions, we vision a Simultaneous Multi-Standard Software Defined Radio (SMS-SDR). An SMS-SDR will be capable of decoding information from multiple heterogeneous wireless standards simultaneously. The capability to receive multiple signals will be made possible by the CCI mitigation techniques. Besides, an SMS-SDR can be customized for new wireless signals by updating the software only. This will be in contrast to Simultaneous Multi-Standard Hardware Defined Radio (SMS-HDR), which will possess the same capabilities as SMS-SDR; however, cannot be programmed for new waveforms.

1.3 Organization of the thesis

- Chapter-2 starts with the discussion on theoretical research and field trials on various interference mitigation techniques. A significant part of our research focuses on developing cross-technology interference mitigation methods. The focus is towards wireless standards in the unmanaged networks in the ISM bands. State-of-the-art architectures of multi-standard SDR platforms follow the discussion.

- Chapter-3 Discusses the details of proposed Simultaneous Multi-Standard SDR (SMS-SDR), associated challenges and our proposed architecture to implement an SMS-SDR.

- Chapter-4 discusses CCI mitigation methods between wideband OFDM and narrowband signals. We chose two typical and popular heterogeneous wireless standards operating in the 2.4 GHz ISM band: IEEE 802.11g and ZigBee. We develop new methods and improvise known methods for single and multi-antenna receivers. Next, we test some selective methods for another pair of wideband OFDM and narrowband signal; IEEE 802.11ax and SC-FDMA to verify the general applicability of the developed methods.

- Chapter-5 discusses CCI mitigation methods between wideband OFDM signals. We chose 20 MHz IEEE 802.11ac and LTE-LAA (LTE with Licensed Assisted Access) which will operate in 5 GHz ISM band and prone to CCI. Likewise chapter-4 we develop new methods and improvise old methods for CCI mitigation in single and multi-antenna receivers.

- Chapter-6 collectively analyze all the signal processing methods developed in chapter-4 and 5. We come up with a decision tree which states the chain of steps to be taken to detect and decode multiple heterogeneous wireless standards simultaneously.

- Chapter-7 provides the details of selective SDR implementations corresponding to chapter-4 and the results of over-the-air (OTA) testing.
- Chapter-8 is the final chapter providing conclusion and future works.

1.4 Published Articles

- Kumar, Sumit; Kaltenberger, Florian; Ramirez, Alejandro; Kloiber, Bernhard: **A WiFi SIC Receiver in the presence of LTE-LAA for Indoor Deployment**. WCNC 2019, IEEE Wireless Communications and Networking Conference,15-18 April 2019, Marrakech, Morocco
- Kumar, Sumit; Kaltenberger, Florian; Ramirez, Alejandro; Kloiber, Bernhard: **Robust OFDM diversity receiver under co-channel narrowband interference** WIMOB 2018, 14th International Conference on Wireless and Mobile Computing, Networking and Communications, 15-17 October 2018, Limassol, Cyprus
- Kumar, Sumit; Kaltenberger, Florian; Ramirez, Alejandro; Kloiber, Bernhard: **A robust decoding method for OFDM systems under multiple co-channel narrowband interferers** EuCNC 2018, 27th European Conference on Networks and Communications, June 18-21, 2018, Ljubljana, Slovenia

1.5 Submitted Articles

- Kumar, Sumit; Kaltenberger, Florian; Ramirez, Alejandro; Kloiber, Bernhard: **An SDR Implementation of WiFi Receiver for Mitigating Multiple Co-Channel ZigBee Interferers** Submitted to EURASIP Journal on Wireless Communications and Networking, Special Issue on "Systems and Networks for 5G Implementation."

1.6 Demonstrations

- Kumar, Sumit; Kaltenberger, Florian: **SDR implementation of narrow-band interference mitigation in wide-band OFDM systems** SPAWC 2018, 19th IEEE International Workshop on Signal Processing Advances in Wireless Communications, 25-28 June 2018, Kalamata, Greece
- Kumit, Sumar; Kaltenberger, Florian: **Mitigating multiple narrowband interferers in SDR IEEE 802.11g diversity receiver** ACM MobiCom 2018, 24th Annual International Conference on Mobile Computing and Networking, 29 October-2 November 2018, New Delhi, India

Chapter 2

Simultaneous Multi-Standard Software Defined Radio

Our prime objective in this thesis is to develop the architecture for an SDR which is capable of detecting and decoding *multiple heterogeneous signals simultaneously*. Our networks of interest are random access networks where homogeneous/heterogeneous wireless standards operate on a shared channel and compete among themselves to capture the transmission medium. In this chapter, we start our discussion with the envisioned functionalities of the proposed Simultaneous Multi-Standard SDR. We continue the discussion with the associated implementation challenges and finally, we present our proposed architecture for an SMS-SDR.

2.1 SMS-SDR

The SMS-SDR we have envisioned will be capable of detecting and decoding multiple wireless signals simultaneously. The signals could be homogeneous, i.e., belonging to the same standard as well as heterogeneous, i.e., belonging to different standards. The architecture is in contrast to the current state-of-the-art in SDR architecture which primarily focuses on reconfigurability and reusability of the hardware and software signal processing blocks. A plausible and oversimplified illustration of General Purpose Processor (GPP) based SMS-SDR is shown in Fig. 2.1. It consists of a single Radio Frequency front-end (RF front-end) which is responsible for low noise amplification followed by intermediate frequency translation, bandpass filtering and finally Analog to Digital Conversion. The digitized signal after ADC is sent to FPGA where the signal is further down-converted and decimated

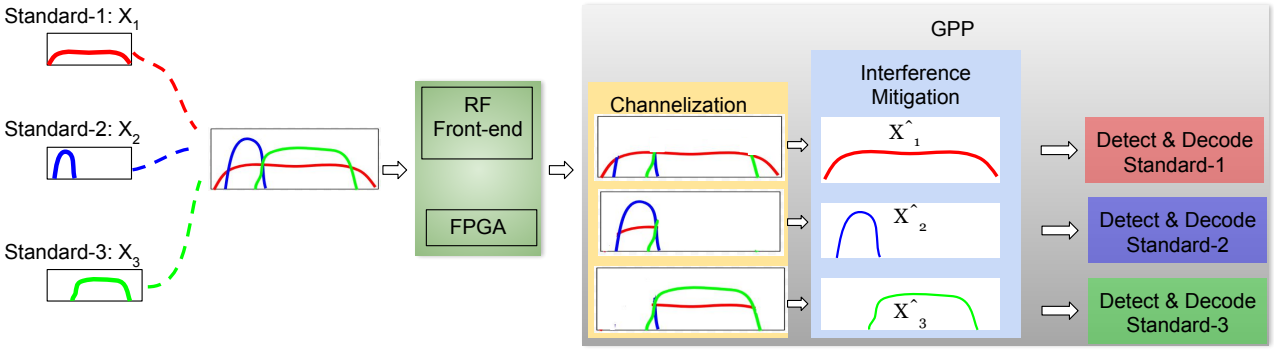


Fig. 2.1. A plausible schematic of a Simultaneous Multi-Standard SDR (SMS-SDR)

for sending the samples via USB or PCI port to the GPP.

We consider a random access network consisting on three different wireless standards: *Standard-1, Standard-2*, and *Standard-3* and the corresponding signals being X_1, X_2 and X_3 respectively [1]. The mentioned standards share the medium of transmission, i.e., they operate on same frequency bands; however, to avoid interference they follow Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [63]. CSMA/CA is based on energy detection of the radiated energy, and we will see later in this chapter that under hidden terminal and blind terminal scenarios, CSMA/CA fails, and transmitted frames from different nodes interfere with each other. In our work, we target such scenarios of interference where CSMA/CA fails and multiple signals arrive at the receiver RF front-end simultaneously. The other case, i.e., when CSMA/CA can avoid interference, is trivial to solve as the signals will arrive at receiver one by one and can be detected and decoded.

Let's assume a collision has happened, and as a consequence, $X_1 + X_2 + X_3$ arrives at the RF front-end through the antenna. The coarse operation of an SMS-SDR consist of the following steps:

- **Step-1:** Wideband sampling at the RF front end such that all the signals of interest are captured. The sampled signal contains a mixture of X_1, X_2 and X_3.

- **Step-2:** The sampled signal is sent to Channelizer in the GPP[2]. A Channelizer is used to extract discrete communication channels located within a wideband signal. In our case, the three signals have different bandwidths, so the Channelizer carves each of them out.

- **Step-3:** The next step is interference mitigation. As we see that our signals overlap each other during concurrent operation, thus, before the signals are sent to their respective receivers, the interference caused by other signals have to be cleaned. Successful operation of interference mitigation yields detectable and decodable estimates $\hat{X}_1, \hat{X}_2$ and $\hat{X}_3$.

- **Step-4:** The estimates are further sent to their corresponding receiver chain for detection and decoding.

The operation of SMS-SDR will be steered by many factors such as the number of antennas at the receiver; received power levels, bandwidth, the modulation scheme of the signals; receiver mobility, etc. The following sections discuss the challenges associated in implementing an SMS-SDR.

2.2 Challenges in Implementing SMS-SDR

The SMS-SDR will use a single RF front-end to capture multiple heterogeneous wireless signals. Heterogeneous signals could be characterized by different modulation schemes, received power level, sampling rates, bandwidths and center frequencies. Capturing signals with such wide disparity in their physical layer characteristics using single RF front-end presents several challenges. A majority of such challenges are related to the hardware begin used in an SDR such as Analog to Digital Converter (ADC) and Channelizer. However, the impairment caused by hardware can be compensated to a large extent in the GPP by applying signal processing software routines.

[1] For the sake of simplicity, we are omitting the channels and use whenever required

[2] Channelizer can be implemented either in the FPGA or GPP

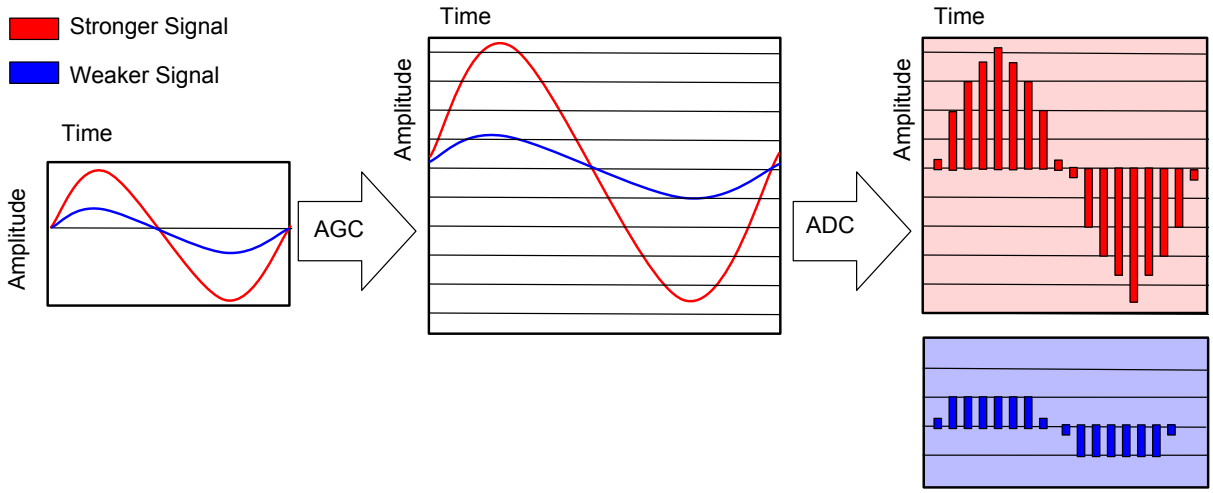


Fig. 2.2. Due to finite ADC bitwidth/resolution, the weaker signal cannot span through the entire dynamic range of the ADC in the presence of a stronger signal. This results in noise like representation of the weaker signal after digitization.

2.2.1 Finite ADC bit width

Different wireless standards arrive at the RF front-end with different received power levels. Any signal arriving at the receiver first goes through Automatic Gain Control (AGC) which amplifies/reduces the signal strength to span the entire range of ADC. In simpler words, AGC is performed so that weak signal does not fall below the noise floor of ADC and the strong signal does not clip off and saturates the ADC. If one of the many heterogeneous standards is significantly louder than others, a higher resolution ADC will be required to capture the weaker signal. Reason being even after AGC, the weaker signal may not be able to utilize the full resolution of the ADC. As shown in Fig. 2.2, with less number of bits used to represent discrete samples of the weaker signal, in the worst case, the weaker signal may appear as single bit noise after the digitization. Once the weaker signal becomes noise like, it cannot be recovered with any signal processing technique. There could be three solutions to this problem:

- Two separate RF front-ends with their AGCs configured for the stronger and weaker signals respectively can be used to preserve the weaker signal; however, plugging as many RF front-ends as the number of signals is not practical.
- Using very high-resolution ADC so that even with low gain by AGC, the weaker signal is represented by as many bits as possible; however, the cost of AGC rises with the resolution.
- The weaker signal fades away in the quantization noise AGC is not able to sufficiently amplify it because doing so will introduce clipping noise in the stronger signal. If the dynamic range of ADC can be increased without inducing clipping noise, it may help the weaker signal to utilize a few more bits. Ulbricht *et al.* in [93] proposed to apply diversity techniques using multiple ADC to which improves the dynamic range of the ADC of a given bit width. According to them, using multiple ADC of equal bit width can be used to overcome the inaccuracy and distortion caused by using a single ADC of the same bit width. Cruz *et al.* in [31] proposed another parallel ADC based solution which increases the dynamic range of the ADC by decreasing the clipping noise. However, both the solutions require changes in the hardware and may not be of much interest if Commercial Off the Shelf (COTS) hardware is being used for development.

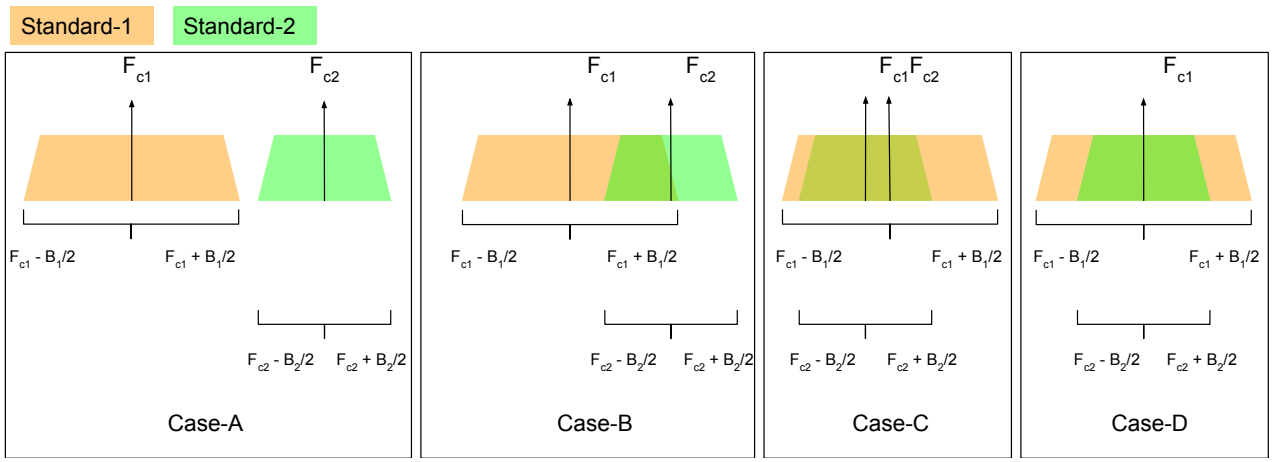


Fig. 2.3. Frequency domain overlap of signals during CCI

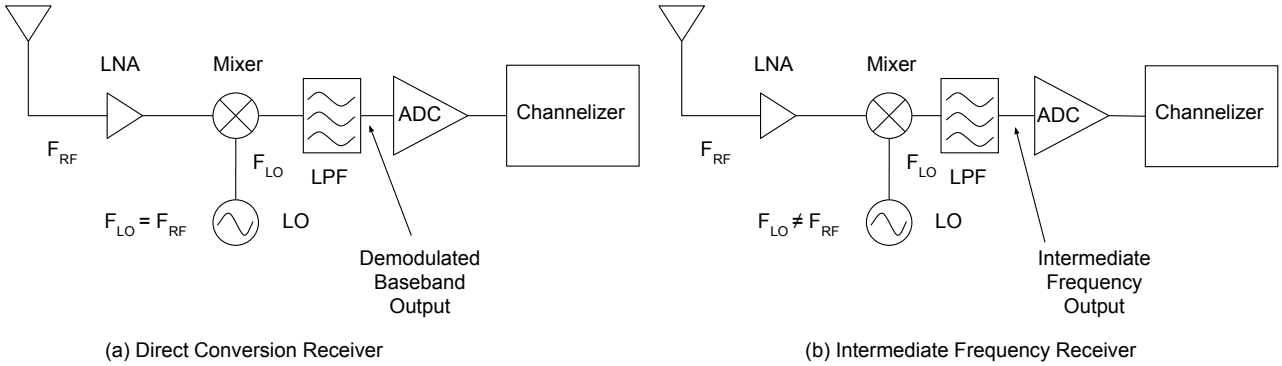


Fig. 2.4. (a) Direct Conversion Receiver (b) Intermediate Frequency Receiver

2.2.2 Channelization

Channelizer is an integral component of SMS-SDR and which helps in extracting narrowband channels from the received wideband signal. A *Channelizer* is responsible to perform channelization and it can be implemented in both FPGA [13] as well GPP [16]. As discussed previously, the heterogeneous wireless signals digitized by the RF front-end of an SMS-SDR could have different bandwidths and different center frequencies. To detect and decode every signal with their respective receivers, the signals need to be translated to their respective center frequencies and bandpass filtered. For illustration, a case of two different signals with center frequencies F_{C1} and F_{C2} and bandwidths B_1 and B_2 respectively is shown in Fig. 2.3. There could be four different cases: One where signals do not overlap in frequency (Case-A) and three other cases where signals overlap in frequency (Case-B, C and D). Nevertheless, in all the cases, the RF front-end tunes its Local Oscillator to $(F_{C1} + F_{C2})/2$ and ADC samples at $F_{C2} + B_2/2 - F_{C1} + B_1/2$ samples per second in order to digitize the entire bandwidth of interest. Now, the digitized signal is passed through bandpass filter of bandwidth $B1$ to carve out a signal belonging to standard-1 and bandpass filter of bandwidth $B2$ to carve out a signal belonging to standard-2.

A Channelizer for SMS-SDR faces the same challenges as the Channelizer of a normal multi-standard SDR (MS-SDR). Because the ability to extract multiple communications channels from a wideband received signal per RF front-end is a fundamental process for any wideband SDR platform. Some of the critical challenges are discussed as follows:

- **Sampling Rate:** RF front-end of any SDR platform is either based on Intermediate Frequency

(IF) or Direct Conversion (DC)[3] receiver architecture. An oversimplified architecture of a single channel IF and DC receiver are shown in Fig. 2.4(a) and Fig. 2.4(b) respectively. Let the IF be F MHz, then for a given bandwidth B of the signal, the sampling rate of ADC in IF receiver is $2 * (F + B/2)$ while the sampling rate of ADC in DC receiver is B only. As the Channelizer is directly connected to ADC in both the receiver, it has to consume samples at the same rate at which the ADC produces.

- **Spectral Content of the Wideband Channel:** Frequency allocation plan and the bandwidths of the wireless standards also drive the complexity of Channelizer. For example, in GSM900 standard both uplink and downlink bands contain 124 channels spaced 200 kHz apart. A channelizer for this case may be able to exploit the redundancy of channel structure and provide an efficient channelization mechanism at lower complexity. However, SMS-SDR is required to channelize many wireless standards which may have non-uniform center frequency allocations as well as bandwidths, for example, WiFi (20 MHz wide and spaced 25 MHz apart) and ZigBee (2 MHz wide and spaced 5 MHz apart) in 2.4 GHz band as shown in Fig. 4.7. The Channelizer employed in SMS-SDR must be flexible enough to accommodate all the carrier/bandwidth combinations. Besides the interoperability of the Channelizer with heterogeneous wireless standards requires dynamic reconfiguration.

2.2.3 Cross Technology Co-Channel Interference

After digitization and channelization, the separate channels containing signals are sent to their respective receivers where they are passed through the usual processing steps, i.e., Frame Synchronization, Timing Synchronization, Decoding, CRC Check, etc. However, as we know that the wideband signal could contain many heterogeneous signals, possibly overlapped with each other. Such distortion when collocated signals overlap and distort each other is called Co-Channel Interference (CCI), and when the signals belong to heterogeneous standards possessing different physical layer characteristic, the distortion is called Cross Technology Co-Channel Interference (CT-CCI). For example, IEEE 802.11g and ZigBee in the 2.4 GHz band. Successful detection and decoding of the signals will now depend on the Signal to Interference plus Noise Ratio (SINR) of the individual signals. CCI is a long known problem in cellular communication regime where it is tackled using centralized coordination by the base station applying transmit time scheduling and fixed frequency assignments [17]. As our focus is developing SMS-SDR for random access networks, the methods being used in cellular communications cannot be directly applied to our case. Reason being lack of centralized coordination in random access networks and contention based channel usage. Cause and repercussions of CT-CCI are discussed in detail in Chapter 4 and Chapter 5. Recovering all the mutually interfered signals is one of the prime tasks of an SMS-SDR; thus, CT-CCI interference mitigation techniques are required.

2.3 Our Approach to Implement SMS-SDR

Implementing an SMS-SDR presents lot many challenges. In the initial phase of our work, we cornered down the issues which we can address with our set of skills and the available apparatuses. We chose to address CT-CCI. The challenges presented by CT-CCI are comparable to any other challenge we discussed so far. As we go into more depth about CT-CCI in Chapter 4 and Chapter 5, we eventually

[3]Also known as Zero-IF architecture

see the gravity of distortions induced by CT-CCI. Nonetheless, it also provides an opportunity for us to address it with our skill set.

In our work chose to address the issue of CT-CCI between heterogeneous wireless standards because of the following reasons:

- Solving Finite ADC bit width issue required hardware modifications which are out of the scope of our work since we are using COTS hardware for our development.
- Channelization is a generic problem related to all types of SDR. The issues are long known, and several efficient Channelizer structures are available to the date.
- Challenging concerns of CT-CCI persists even after the issues related to finite AC bit width and channelization are solved. CT-CCI may render the signals undetectable and non-decodable even after they have been efficiently digitized and channelized putting all the efforts in vain.
- CT-CCI can be effectively addressed in software without the need for hardware reconfiguration. Addressing CT-CCI in software provides additional flexibility to adapt the techniques for multiple heterogeneous wireless standards.

The first step in our approach to implementing SMS-SDR is the development of a diverse set of CT-CCI mitigating signal processing algorithms. During the development of methods, we particularly stress on the following three things:

1. Compliance with existing commercial transmitters, i.e., detection and decoding of standard-compliant waveforms.
2. Re-usability to many wireless standards with minor modifications.
3. Ease of implementation using COTS SDR hardware and software packages.
4. Required signal processing to be performed only on the receiver side, i.e., without any cooperation with the transmitter as well as any central coordination. In this way, the method is useful for random access networks.

To develop CT-CCI mitigation techniques, we chose practical cases of CT-CCI. We target the random access networks operating in 2.4 GHz and 5 GHz band. We revisit the legacy standards: IEEE 802.11g, ZigBee (based on IEEE 802.15.4), latest standards IEEE 802.11ac, LTE (OFDMA and SC-FDMA) and finally the upcoming standards: IEEE 802.11ax to develop a rich set of CT-CCI mitigation techniques. Although we chose heterogeneous wireless standards with different physical layers, we pay particular attention to standards which use Orthogonal Frequency Division Multiplexing for their physical layer. The reason being OFDM is dominantly used in old/existing/upcoming wireless standards such as IEEE 802.11a/g/n/ac/ax, LTE, DVB-T, DAB, etc. We also focus on developing generic methods which can be applied many standards instead of standard specific methods which limits their applicability. Besides, we also implement several state-of-the-art methods and include them in our set of CT-CCI.

In the next part of our approach is the development of decision trees from the developed CT-CCI methods. To do so, we use the methods developed by us as well as state-of-the-art methods for CT-CCI mitigation. A decision tree decides the appropriate CT-CCI methods and customizes them to mitigate CT-CCI between any two or more given wireless standards. The decision tree also recommends the

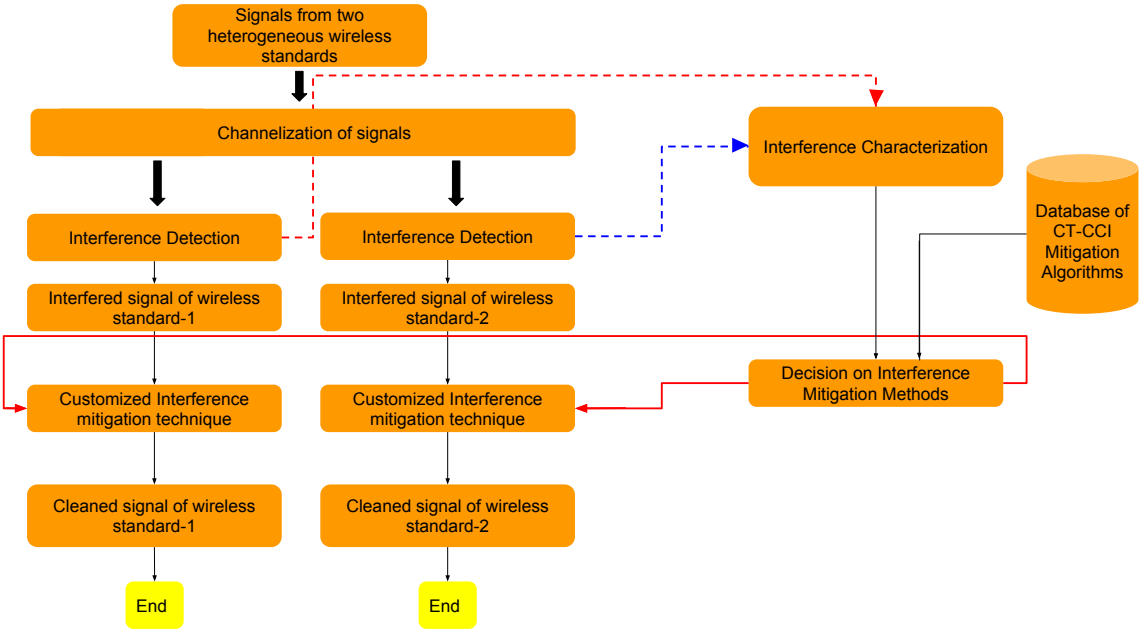


Fig. 2.5. Example flow diagram for mitigating CT-CCI from two heterogeneous wireless standards operating on overlapped frequency bands

chain of steps to be taken for selection of CT-CCI methods. A sample flow diagram which uses a decision tree to mitigate CT-CCI between signals from two heterogeneous wireless standards is shown in Fig. 2.5. Signal captured from wideband RF is first sent for channelization and then interference detection. Further, the type and extent of interference are characterized. Based on the characteristics of interference and the list of CT-CCI algorithms available, CT-CCI techniques are decided and customized. Next, these customized CT-CCI methods are used to mitigate mutual interference from the signals.

We believe that any application developed for SDR is not complete without implementing in and performing over-the-air (OTA) tests. Hence in the final part of our work, we implement some of the selected methods using COTS SDR hardware and SDR software packages. For SDR hardware we chose Ettus B210 USRP and on the software side, we chose two open source programming tools GNU Radio [78] and Openairinterface [51].

Chapter 3

Related Work and State of the Art

This chapter provides a background of the co-channel interference (CCI) mitigation techniques. We primarily examine the physical layer signal processing techniques which follow the decentralized approach, i.e., there is no requirement of a central coordinator. Such methods are suitable for random access networks which are deployed in an unplanned manner such as WiFi, Bluetooth, ZigBee, LTE-LAA. In addition, we discuss recent development on the architecture of multi-standard SDRs.

3.1 Co-Channel Interference

Interference plays a central role in limiting the capacity of the widely proliferated wireless networks. With the evolution of cellular networks, researchers have put significant efforts in developing interference mitigation techniques. But what is the cause of interference? There are many such as:

- When multiple collocated transmitters transmit concurrently on the same medium, the frames overlap over each other, resulting in interference. This is known as Co-Channel Interference (CCI)[33].
- When multiple collocated transmitters transmit concurrently on the different medium; however, the power spills out from one medium to another resulting in interference. This is known as Adjacent Channel Interference (ACI)[33].

As discussed in Section 2.2.3, CCI is one of the dominant challenges to be addressed before an SMS-SDR can be realized; hence we focus on CCI mitigation techniques. Moreover, our focus is towards mitigating CCI among heterogeneous wireless standards whose frequency bands of operation overlap. Nonetheless, we examine the available literature which covers both CCI and CT-CCI as the methods belonging to mitigate CCI can also be applied to CT-CCI with necessary modifications.

The issue of CCI was identified at the very early stage of cellular communications, and most of the solutions resorted towards designing a centralized regulator/coordinator which exclusively granted the medium of communication(time, space, frequency) to a single user at a time [17]. However, such exclusive allocation of the medium resources leads to excessive waste as the users may or may not used the assigned resources depending on the traffic load. With the rise of unlicensed networks such as WiFi, Bluetooth, ZigBee, decentralized approaches of channel access evolved such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), Orthogonal Frequency Division with Multiple Access (OFDMA). With more advances in signal processing methods, techniques such as interference cancellation, interference alignment, interference nulling also came up, all with their pros and cons.

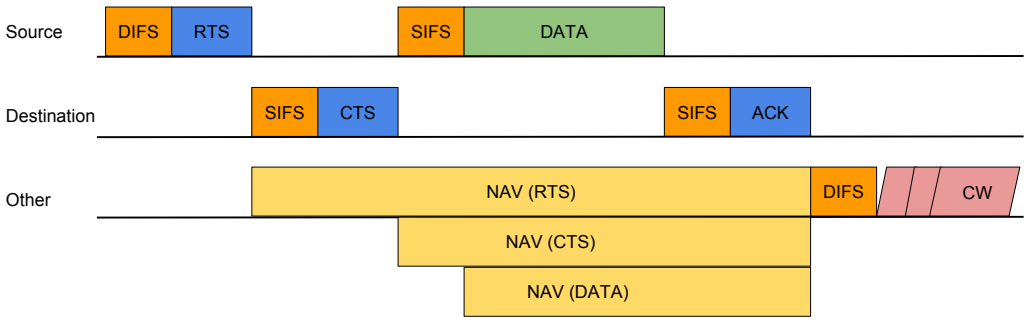


Fig. 3.1. A typical proceedure of CSMA/CA

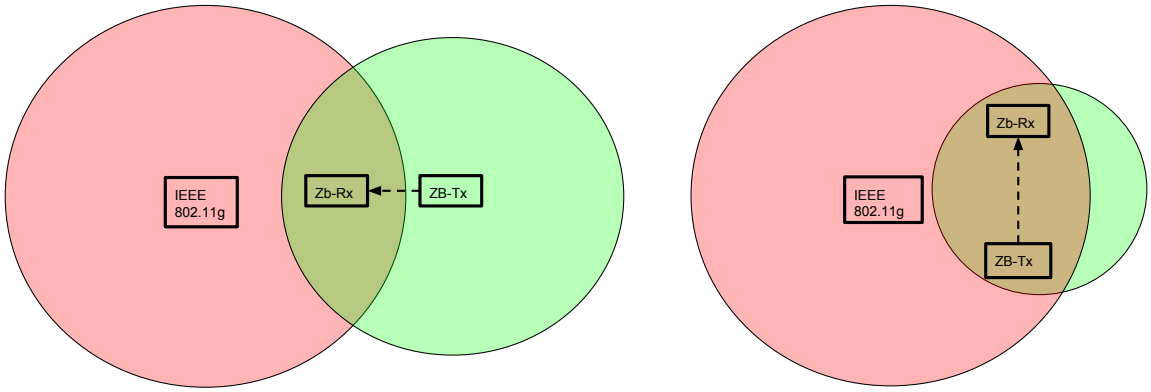
While applying CCI mitigation techniques, cellular networks benefit from the centralized coordination by the base station.

In contrast, the networks operating in the unlicensed bands lack from any such centralized coordination which makes application of CCI mitigation techniques used in cellular communication challenging to apply. Nonetheless, the problem is being investigated since long, and a multitude of methods have been proposed. In the following sections, we discuss the broad classes of CCI and CT-CCI mitigation methods developed for decentralized networks and discuss the relevant state of the art.

3.2 Collision Avoidance

As the name says, such methods aim towards avoiding the collision at the very place. Collision avoidance based approach reserve the medium of communication exclusively for one user at a time; whether the medium is time, frequency or space. The very basic collision avoidance techniques were devised during the early stages of cellular networks by exclusively reserving the transmission medium orchestrated by a centralized coordinator. Some of the basic examples [33] are Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA) and Space Division Multiple Access (SDMA). These methods are instrumental in mitigating CCI; however, looking towards the random access networks such as WiFi, the methods mentioned above cannot be utilized directly as all of them require a centralized controller for orchestrating the reservation the medium.

Random access networks, on the other hand, use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [46], which reserves the medium on a contention basis. CSMA/CA is the de facto mechanism used by all the IEEE 802.11 family and IEEE 802.15.4. Using CSMA, the nodes in the network can detect what is going on in the transmission and if there is no activity, they send their data. In case another node is already using the medium, the sensing node backs off and wait for a random amount of time following an exponential counter and then tries again. CSMA is being used in wired networks for a long time under the name CSMA/CD where CD stands for Collision Detection. Collision Detection is possible in a wired medium but its very hard to detect it in the wireless medium. Thus wireless medium use CSMA/CA which does Collision Avoidance, i.e., prevents collision before they happen. The procedure of CSMA/CA is shown in Fig. 3.1. When a source has



(a) Hidden Terminal (b) Blind Terminal

Fig. 3.2. Hidden and Blind terminal scenarios between IEEE 802.11g and ZigBee

to send data, it senses the channel, if found free, it waits further for DIFS (Distributed Coordination Function Inter Frame Spacing). If the channel is still free, it sends an RTS (Request to Send) packet towards the destination. Upon reception of RTS, the destination waits for SIFS (Short Inter Frame Spacing) and then sends a CTS (confirm to Send) towards the sender. Upon receiving CTS, the sender waits for SIFS and sends the Data. Upon reception of data followed by waiting for SIFS, the destination sends the acknowledgement ACK. During this period all other senders listen to the RTS/CTS packets. RTS/CTS packets have the additional information termed as Network Allocation Vector (NAV) about the air time of prospective payload. Thus upon listening RTS/CTS, other senders defer their transmission. Once the ACk has been sent from the destination, then after waiting for DIFS, the contention to capture the channel starts and the process goes on. In this way, CSMA/CA makes sure that at a given time there is only one transmit-receive pair in the medium.

However, under the situation of *Hidden Terminal* and *Blind Terminal* CSMA/CA is ineffective fails. Let's take an example of IEEE 802.11g and ZigBee. Both operate in the 2.4 GHz ISM band and use CSMA/CA to capture the channel opportunity. In hidden terminal, as shown in Fig. 3.2(a), IEEE 802.11g node cannot listen to the transmission of ZigBee transmitter (ZB-Tx) as it is out of range. Hence both of them assume the channel to be free and start transmitting to the channel at the same time resulting in a collision. Similarly, in the blind terminal, as shown in Fig. 3.2(b), both ZB-Tx and ZB-Rx are inside the interference region of IEEE 802.11g, but IEEE 802.11g is outside the sensing region of ZB-Tx. This again results in simultaneous transmission leading to a collision. According to authors of [82], [91], in a randomly distributed network, the probability of hidden node formation could be as high as 41%. To counter the effects of hidden terminal and blind terminal, Request-To-Send (RTS) and Clear-To-Send (CTS) packets are exchanged between the Tx-Rx pairs in IEEE 802.11g; however, in practice RTS/CTS is disabled in commercial IEEE 802.11g Access Points as they decrease the throughput by 40% [68]. Instead, the transmitter sends the data just after waiting for DIFS once it senses the channel as free. Although CSMA/CA is useful in avoiding the collisions and operate in a decentralized fashion, analysis by Cagalj *et al.* in [28] shows the selfish behavior of CSMA/CA. As the nodes are becoming highly programmable, they are capable of controlling their random backoff duration to provide the users more transmit opportunities at the cost of reduced air time for users playing fair. Konorski [52] also shares the same view about the greedy users who exploit the programmability of nodes and compromise with the exponential back-off scheme.

3.3 Interference Cancellation

Methods belonging to this class exploit the fact that unlike noise, which is stochastic, interference is deterministic. Deterministic nature of interference presents the possibility to decode the interfering signal! Since the received signal after interference is a sum of the desired signal and interfering signal, the decoded interference can be subtracted from the received signal to obtain the desired signal. Interference cancellation is a multi-step process and commonly known as Successive Interference Cancellation (SIC)[70][97].

Current cellular networks are already practicing SIC; however, they benefit from centralized control over hardware, power, rate, synchronized transmitters. Halperin *et al.* implemented a working prototype of SIC in random access networks in [39] where the physical layer of IEEE 802.15.4 along with SIC modules was implemented on a USRP SDR. Their implementation used BPSK where SINR requirement for decoding is relatively low. For dense constellations, their simplistic approach may face significant challenges. Tan *et al.* performed SDR implementation of SIC for uplink using Microsoft SORA SDR[88]. The process requires coordination between the participating transmitters followed by SIC of unwanted signals at the access point. Another notable work of SIC was done by Golakota *et al.* termed as Zig-Zag decoding in [36]. A Zig-Zag system exploits the fact that two packets which have collided are likely to collide again as the senders will attempt to transmit them again, but during the next collision, the frame overlap will be different because of the random backoff. The receiver can store and use different versions of the same frame in a block by block manner. This is suitable for IEEE 802.11 networks which apply CSMA/CA. However, Zig-Zag is suitable when the packets from two different transmitters are destined to the same receiver, for example, multiple clients to the same access point. With different destinations of different frames, the collision of the same frames is not guaranteed.

SIC is one of the proven methods to increases the capacity of the wireless network by allowing concurrent transmissions on a shared medium. On the downside, SIC techniques require a difference in power levels of the competing signals and are not effective when the signals arrive with a comparable difference in power. Besides, a high power signal can saturate the receive amplifier making it deaf towards the weaker signal.

3.4 Directional Antennas

One of the major reasons of interference is the widespread application of omnidirectional antennas which not only transmit towards the destined receiver but everywhere else too. For example dipole antennas whose radiation pattern is omnidirectional in azimuth as shown in (left)Fig. 3.3. However, there is another class of antennas called directional antennas which have high gain in one or more directions and low in other as shown in (right) Fig. 3.3. The gain pattern depends on the antenna geometry as well as operating frequency.

Directional antennas can be very useful in limiting the interference. With directional antennas, independent communications between nodes can occur in parallel, even if the nodes are within range of each other. Babich *et al.* in [21] examined the performance of directional, switched beam and adaptive antennas while applying them in a distributed IEEE 802.11 network. They combined the application of directional antennas along with an aggressive approach during CSMA/CA and suggested to reduce the duration of the minimum contention window for the efficient exploitation directional

antennas. Giorgetti *et al.* proposed multi-beam directional antenna for 2.4 GHz IEEE 802.15.4 motes to mitigate interference caused by IEEE 802.11 nodes. They performed field trials using fabricated multi-beam directional antenna and COTS motes and registered 70% in reduction. Besides, the range of the motes was extended by more than 100 meters. In another experiment, Vangelis *et al.* in [18] showed the application of directional antennas to reduce adjacent channel interference in IEEE 802.11a. Although the use of directional antennas can improve the system performance by avoiding

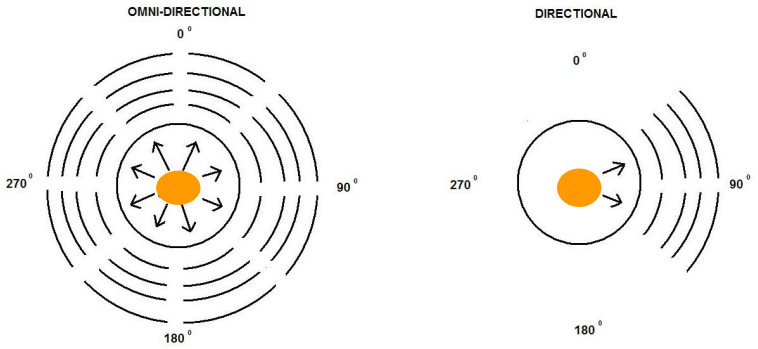


Fig. 3.3. Radiation pattern of omni directional and directional antennas

interference, on the downside, the system loses its capability of broadcast behavior. Christopher *et al.* in their patent [30] came up with a solution to improve the functionality of directional antennas for random access networks. The patent suggested applying omnidirectional antenna for broadcast messages and directional antennas for point-to-point links. Tamer in [73] analyzed the reduction in spatial reuse due to directional antennas.

The other downside of directional antennas is fixed beam pattern or fixed direction. Hence, for the given setting, if the directional antenna is performing excellent, there is no guarantee that it will continue to perform well in other environments too. To address the issue, the idea of switched beam antennas came up. Such antennas can change their beam patterns in contrast to the fixed beam patterns of the directional antennas. Switched beam antenna contains multiple antenna elements, and by changing the amplitude and phase to the feeds, the beam pattern can be varied. Ahn *et al.* in [15] experimented the application of switched beam antennas to avoid interference in IEEE 802.11b network. The proposed system was capable of tracking the direction of incoming interference and creating null towards it.

3.5 Interference Nulling

Multiple antenna systems have become de facto standard in modern and upcoming wireless communication systems, for example, IEEE 802.11n/ac/ax and LTE-A. They use the principles of Multiple Input Multiple Output (MIMO) to send several streams of information in parallel. Although the prime motive of MIMO systems has been data rate increment, nonetheless they can be used to null the interference.

History of nulling co-channel interference using multiple antenna backs to the historic paper by Winters *et al.* [98]. Authors proposed Optimal Combiner (OC) which uses N available antennas at the receiver to cancel N-1 co-channel interferers. In Chapter 4 we discuss the details of OC and through simulations show that OC none of the interference nulling mechanism can achieve better per-

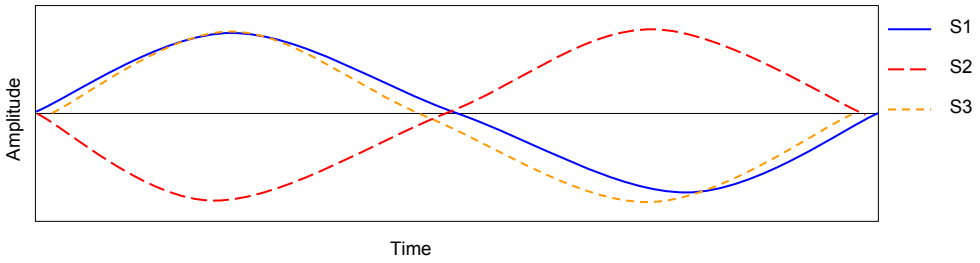


Fig. 3.4. Constructive and destructive addition of same signal coming from different paths

formance than OC. OC attempts to maximize the SINR of the signal in the presence of colored noise. However, OC requires Interference Plus Noise correlation matrix for its operation, the complexity of computation of which grows as the number of antennas grow. Such requirements prevent the practical implementation of OC as a mean to nullify the interference.

For interference nulling, modern MIMO systems exploit the fact that the same signal received by different antennas at the receiver is subjected to different paths and hence different attenuations and phase. Thus, if different versions of the same signal are aligned in a particular manner, the combined signal could be either amplified or attenuated version of the original signal. For example, Fig. 3.4 shows three versions of the same transmitted signal. If a two antenna receiver receives $S1$ and $S2$, the resulting combination will be a weaker signal than the transmitted one. On the other hand, if received, the combination of $S1$ and $S3$ will boost up the signal. If the receiver is capable of aligning the phase of the received signals, the above two cases could be used to boost the desired signal and nullify the interference; the method is also called Interference Alignment (IA), and some of the notable early works include Jafar *et al.* in [27] and Wolniansky *et al.* in [99]. The former applies Interference Alignment (IA) to compute the degree of freedom a MIMO system can achieve while the later applies IA to decode multiple streams simultaneously. In another landmark work, Shyamnath *et al.* proposed IAC (Interference Alignment and Cancellation) in [35]. The scenario they considered was uplink, and the transmitters chose their respective phases to facilitate alignment at the receiver. Their set-up requires a central coordinator and is suitable for enterprise WLAN.

In contrast, Lin *et al.* in [63] proposed a decentralized system for IEEE 802.11n systems which was capable of aligning the simultaneous transmissions and nulling them at the receiver. OpenRF, an interference nulling system was proposed by Kumar *et al.* in [57] uses commodity WLAN cards to perform interference alignment and nulling. However, their system needs a centralized controller and which synchronizes all the transmitter willing to transmit simultaneously.

All the interference nulling techniques require the channel estimates of the interferer (channel between the interfering transmitter and the receiver). With cross-technology wireless standards operating in random access networks, it is very challenging to obtain a clean channel estimate of the interferer. Gollakota *et al.* in [34] proposed Technology Independent MIMO (TIMO). A TIMO receiver performs the traditional receive beamforming to null the interference without the knowledge of the exact channel estimates of the interferer. Instead, TIMO uses the ratio of the channel estimates of the interfere on the two antennas of the receiver. The method is suitable to mitigate CT-CCI as it is difficult to guarantee the accurate channel estimates of the interferer. Hou *et al.* in [45] extended the technique of TIMO for multi-hop wireless networks where nodes mutually co-operate to cancel the interference to each other.

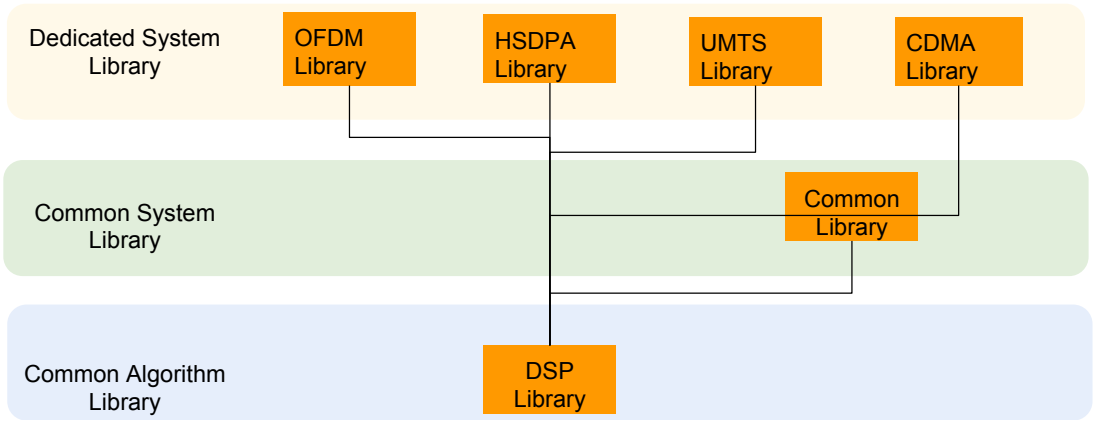


Fig. 3.5. Method for multi-standard software defined radio base-band processing [65]

3.6 Multi-Standard Software Defined Radio

In this section, we discuss research related to multi-standard SDR. Most of the research work of multi-standard SDR focus on reconfigurability and they reuse the software and hardware components. In this way, they realize waveforms corresponding to multiple wireless standards. Authors in [22] propose solutions for a generic GPP based SDR architecture that can be used to implement smart multi-standard SDR terminals where the hardware of the terminal is fixed. The proposed architecture is used to generalize the implementation of the WLAN protocol. For example, some blocks are common for different standards with similar transmission method. For instance, FFT/IFTT, pilot insertion, guard interval, and OFDM symbol assembler, convolution encoder, and Viterbi decoder are used in OFDM based systems such as WLAN, Digital Video Broadcasting (DVB), and World Interoperability for Microwave Access (WiMAX).

Authors in [79] discuss dynamic reconfiguration of FPGA based SDR platforms termed as Dynamic Partial Reconfiguration (DPR) technique. They investigate the similarity between 2G, 3G, LTE and WiFi such as: Channel Coding(3G: R=1/2, K=9 and R=1/3, K=9, LTE: R=1/3, K=7, WiFi: R=1/3, K=7), Puncturing, Interleaving, QAM Mapping/Demapping, FFT/IFFT (WiFi: 64 and LTE: 256) etc and exploit those similarities to come up with common signal processing blocks which can be used to implement most of the waveforms on an FPGA based SDR platform.

Authors in [77] develop a mathematical model to determine an optimal architecture for a multi-standard reconfigurable radio. They examine the well known Velcro approach which consists of self-contained complex but dedicated components for every standard and compare it with smaller and simple components. They come up with a simpler architecture which uses simple lower-level components for reconfiguration of multi-standard SDR. They term their approach as parametrization and primarily focuses on reducing the reconfiguration latency using simpler components.

In the patent [65] by Luo *et al.* , a method for the baseband processing of multi-standard SDR is discussed. The method divides the SDR baseband processing units as dedicated system libraries, common system libraries and DSP libraries as illustrated in Fig. 3.5. Their architecture provides the capability to reprogram, the capability of providing and changing services and finally capability to support multiple standards. Although, the architecture does not talk about simultaneous operation over multiple wireless standards; nonetheless it can be used as a template architecture for our proposed SMS-SDR.

Table 3.1: Relative Comparison of CCI and CT-CCI Mitigation Techniques

	CSMA/CA	**Successive Interference Cancellation**	**Interference Alignment**	**Directional Antennas**
Standalone Processing at the Receiver	Yes	Yes	No	Yes
Need for Centralized Controller	No	No	Yes/No	No
Cross technology	Yes	Yes	Yes	Yes
Suitable for Random Access Networks	Yes	Yes	Yes	Yes
Implementation Complexity	Low	Medium	Medium	High (Hardware is bulky compared to omni-directional antennas)

3.7 Summary

Ubiquitous deployment of wireless networks and growing demand for capacity is continuously pushing the research community to address the interference in new and innovative methods. Each method comes with its pros and cons. Collision avoidance is the most intuitive way, but it often leaves the allocated resources unused. SIC produces promising results in simulations, but the effectiveness fades away in practical SINR scenarios, especially without any control over the transmit power. Interference nulling are relatively easy to implement but require coordination from the transmitter to precode the users who wish to transmit simultaneously. Finally, the directional antennas are instrumental in mitigating CCI plus they extend the range also, however, they are bulky to integrate with small devices. A table containing the relative comparisons of CCI and CT-CCI mitigation methods is shown in Table 3.1.

The current architecture of multi-standard SDR focuses mainly on reconfiguration and reusability of the signal processing blocks to realize many wireless waveforms. Although the current architectures do not address simultaneous operation of more than one wireless standard, nonetheless, the current architectures can be piggybacked along with suitable CT-CCI mitigation techniques to realize an SMS-SDR.

Chapter 4

CT-CCI Mitigation Between Wideband OFDM and Narrowband Signals

This chapter discusses the CT-CCI between wideband OFDM signals and narrowband signals. We start our discussion with IEEE 802.11g as the wideband OFDM signal and ZigBee as the narrowband signal and develop CT-CCI mitigation methods followed by verification of their performance through simulation experiments. Further, we test our methods for the case of CT-CCI between wideband IEEE 802.11ax(which is also a wideband OFDM signal) and another narrowband signal based on SC-FDMA. Results of our simulation experiments show that the methods developed by us can be generalized for the case of CT-CCI between any wideband OFDM and narrowband signal. We prototype both single and multi-antenna receivers in our methods.

4.1 Physical Layer of IEEE 802.11g and ZigBee

The 2.4 GHz band is being long dominated by the IEEE 802.11 family (popularly known as *WiFi*) such as IEEE 802.11n, IEEE 802.11b and IEEE 802.11g. WiFi operates efficiently without the need of any centralized coordination and with minimal set-up time. No wonder it is one of the most popular wireless standards which has survived two decades in both home and commercial set-ups. ZigBee [84] is another robust wireless standard primarily used for low power and low rate communications such as wireless sensor networks. ZigBee is based on IEEE 802.15.4 and operates in 868 MHz, 915 MHz, and 2.4 GHz band. The physical layer of IEEE 802.11g and ZigBee are completely different, and so is their receiver structure.

4.1.1 IEEE 802.11g

IEEE 802.11g was induced in 2003 [46]. It operates in 2.4 GHz ISM band with a peak throughput of 54 Mbps. It has been categorized under Non-High Throughput (Non-HT) category because compared to the recent IEEE standards such as IEEE 802.11n (HT: High Throughput), IEEE 802.11ac(VHT: Very High Throughput), the data rate of IEEE 802.11g is less. IEEE 802.11g is based on OFDM and uses 64 point FFT generating 64 overlapping yet orthogonal OFDM subcarriers. Subcarrier allocation within one OFDM symbol for IEEE 802.11g is shown in Fig. 4.1. Out of 64 subcarriers, 48 subcarriers

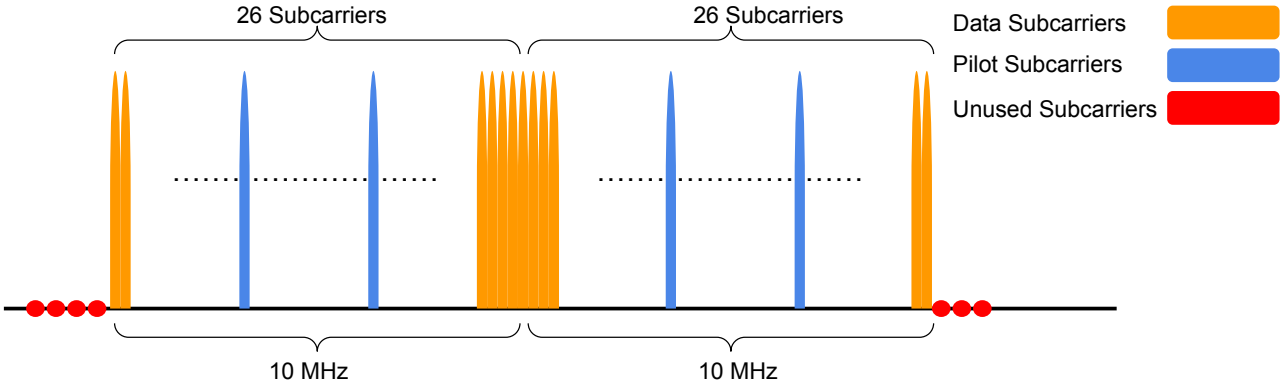


Fig. 4.1. IEEE 802.11g Subcarrier Allocation

L-STF	L-LTF	L-SIG	SERVICE bits	Payload	Pad bits	Tail bits

Fig. 4.2. IEEE 802.11g Non-HT frame format

are used for data, 4 subcarriers as pilots and rest 11 subcarriers are unused to help isolate against adjacent channel interference. Pilot subcarriers are used for phase correction in the OFDM data symbols. Additionally, the DC subcarrier at the center is left unused to avoid DC leakage caused by the usage of low-cost Direct conversion receivers. All the 48 data subcarriers are modulated with the same modulation scheme. Supported modulation schemes in IEEE 802.11g are BPSK, QPSK, 16QAM, and 64QAM. Frame format of IEEE 802.11g is shown in Fig. 4.2. L-STF stands for *Legacy Short Training Frame* and used for incoming frame detection, coarse frequency offset correction and automatic gain control. L-LTF stands for *Legacy Long Training Frame* and used for symbol timing offset correction, fine frequency offset correction, noise variance estimation, and channel estimation. L-SIG is the *Legacy SIGNAL field* which contains information such as the modulation scheme used for the payload, payload length, etc. L-SIG is always modulated using BPSK regardless of the modulation used for payload. The payload contains the actual data to be transmitted. IEEE 802.11g uses CSMA/CA for accessing the channel and avoiding collision.

4.1.2 ZigBee

ZigBee was conceived in 1998 and standardized in 2003 [41]. ZigBee is intended for low-throughput, low-power, and low-cost applications. The 2.4 GHz ZigBee uses Offset Quadrature Phase Shift Keying (O-QPSK) and Direct Sequence Spread Spectrum (DSSS) as the modulation scheme. In our work, we have chosen 2.4 GHz ZigBee as IEEE 802.11g also operates in the same 2.4 GHz band and causes CT-CCI. ZigBee uses IEEE 802.15.4 for its PHY and MAC while adds its propriety architecture for the higher layers as illustrated in Fig. 4.3. Frame format of a typical ZigBee frame is shown in Fig. 4.4 The preamble consists of 8 zeros which are used for frame detection, Start of Frame Delimiter (SFD), always set to 0X7A, is used to find the start of a packet, PHY header contains the length of the payload which is the next field in the frame. Binary data coming from the application layers is first spread using 16-ary orthogonal modulation using a set of orthogonal 32-bit chip sequence. Spreading sequences yield multipath and ISI resistance. The resulting bit sequence is further modulated using O-QPSK giving a baseband bandwidth of 2 MHz. Receiver sensitivity of ZigBee (Packet Error Rate

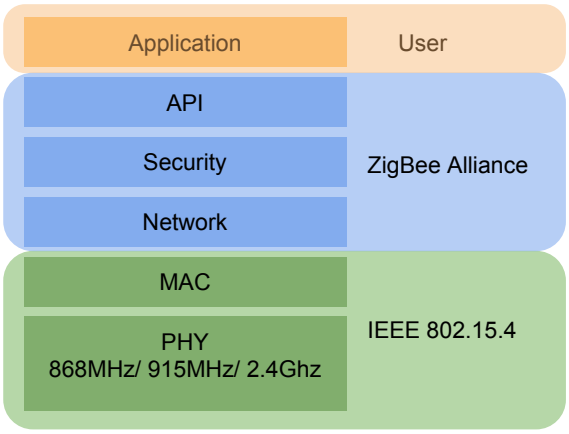


Fig. 4.3. ZigBee OSI Architecture

Preamble	Start of Frame Delimiter	PHY Header	Payload

Fig. 4.4. ZigBee Frame Format

$< 1\%$) is -85 dBm in 2.4 GHz ISM band. Likewise IEEE 802.11g, ZigBee also uses CSMA/CA for accessing the channel and avoiding interference [102].

4.1.3 Interference Scenarios

The root of CT-CCI between IEEE 802.11g and ZigBee arises due to their frequency allocation in the 2.4 GHz band as shown in Fig. 4.5 and Fig. 4.6. We see that IEEE 802.11g spans over 80 MHz within which it has 14 channels, each 20 MHz wide; however at a given location and time only 3 of them can operate in a non-overlapping manner. For example channel-$1, 6$ and 11. Channel-14 is not commonly used (used only in Japan). In the same 2.4 GHz band ZigBee also spans over the entire 80 MHz band comprising of 16 non-overlapping channels each 2 MHz and frequency spacing of 5 MHz. While all the IEEE 802.11g channels overlap with at least one or maximum four ZigBee channels, ZigBee channel $4, 9, 15$ and 16 are free from interference as shown in Fig. 4.7. Both IEEE 802.11g and ZigBee use CSMA/CA for accessing the channel on the same frequency band. CSMA/CA is based on energy detection where the transmitters sample the channel and compute the energy. If the energy exceeds a predefined threshold, the channel is marked busy and the transmission time is deferred according to an exponential backoff algorithm. The CSMA/CA mechanism works effectively even if the wireless standards are different, i.e., IEEE 802.11g can defer its transmission when ZigBee is transmitting on the same channel and vice-versa. However, in the situation of *Hidden Terminal* and *Blind Terminal* as discussed in Section 3.2, CSMA/CA is ineffective. Especially the heterogeneity in power level of IEEE 802.11g and ZigBee can readily cause hidden terminal problem [104]. Within an IEEE 802.11g networks, the problem of the hidden and blind terminal is solved using the exchange of RTS-CTS packets at the cost of reduced throughput[104];however there is no provision of such mechanism between IEEE 802.11g and ZigBee. Going into the granular details of interference, for IEEE 802.11g, the interference caused by ZigBee appears as frequency selective noise which is higher on some of the subcarriers while lower on some of the subcarriers. For example, when a single ZigBee channel overlaps with a single IEEE 802.11g channel, 20 MHz / 2 MHz, i.e., ≈ 7 subcarriers of IEEE

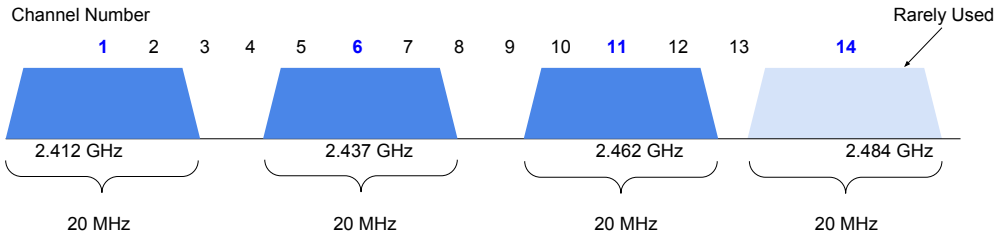


Fig. 4.5. Frequency Allocation of IEEE 802.11g in 2.4 GHz band

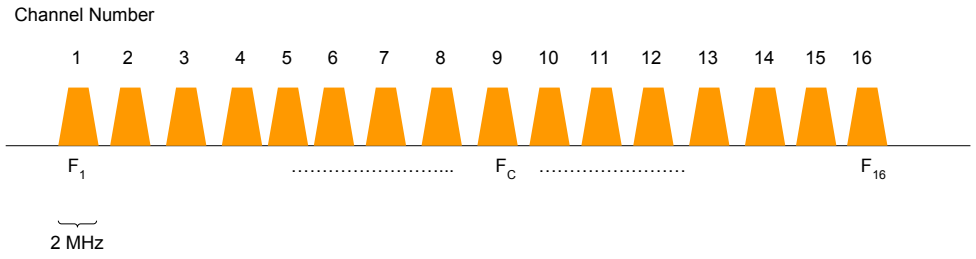


Fig. 4.6. Frequency Allocation of ZigBee in 2.4 GHz band

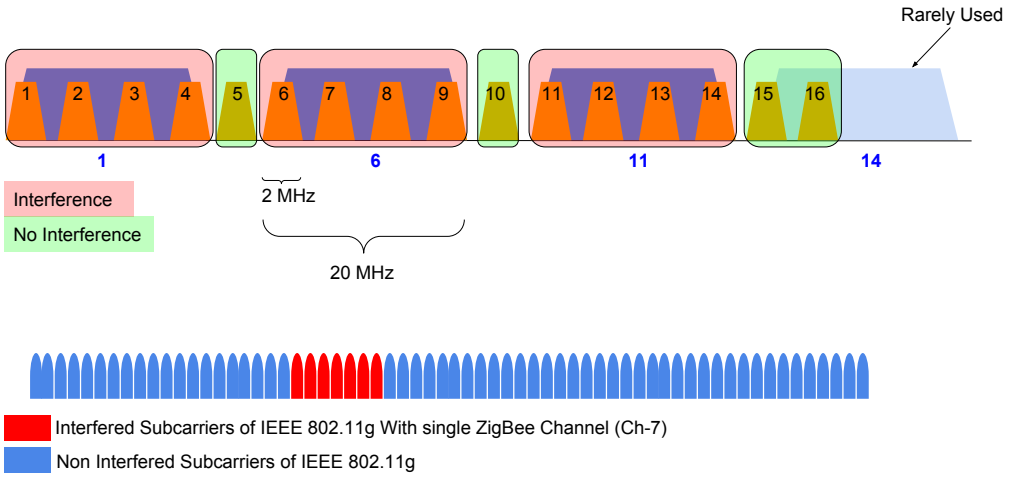


Fig. 4.7. IEEE 802.11g and ZigBee overlap

802.11g (marked red in bottom of Fig. 4.7) get affected. To have an estimate of the performance degradation of IEEE 802.11g caused by ZigBee, we performed a simulation of interference between single antenna IEEE 802.11g receiver and interfered by fixed power single antenna ZigBee transmitter (−85 dBm). [1]. The Packet Error Rate (PER) is plotted in Fig. 4.8 which indicates severe degradation of IEEE 802.11g PER for all the MCS which agree with the previous simulations and field trials. On the other hand, the interference of IEEE 802.11g to ZigBee appears as frequency flat noise. To assess the performance degradation of ZigBee caused by IEEE 802.11g, we performed simulations of interference at a fixed IEEE 802.11g Transmit power of −85 dBm, MCS 0 and varying ZigBee power with same simulation parameters as mentioned above. PER is plotted in Fig. 4.9 which again agree with the previous studies.

In the event of CCI between IEEE 802.11g and ZigBee, an SMS-SDR is required to recover both IEEE 802.11g and ZigBee from the collided packets it receives. In the coming sections, we develop

[1]Noise power = −100 dBm, 11 tap Rayleigh fading channel with exponentially decaying power delay profile for IEEE 802.11g and single tap Rayleigh channel for ZigBee

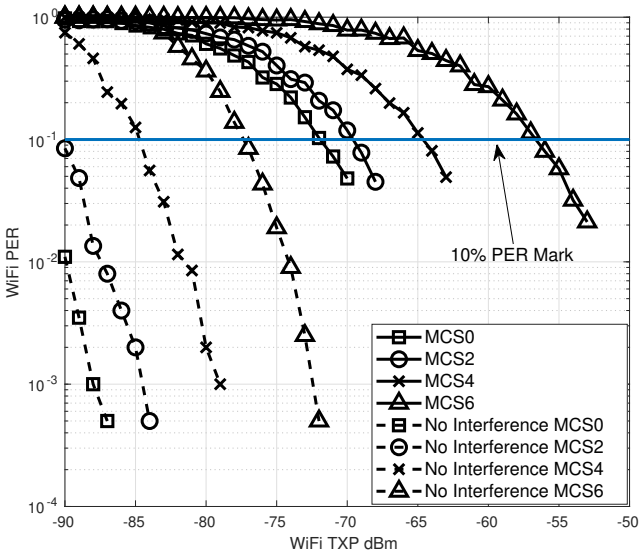


Fig. 4.8. PER of single antenna WiFi receiver in the presence and absence of single antenna ZigBee transmitter(transmit power -85 dBm). For all IEEE 802.11g MCS, we observe severe PER degradation.

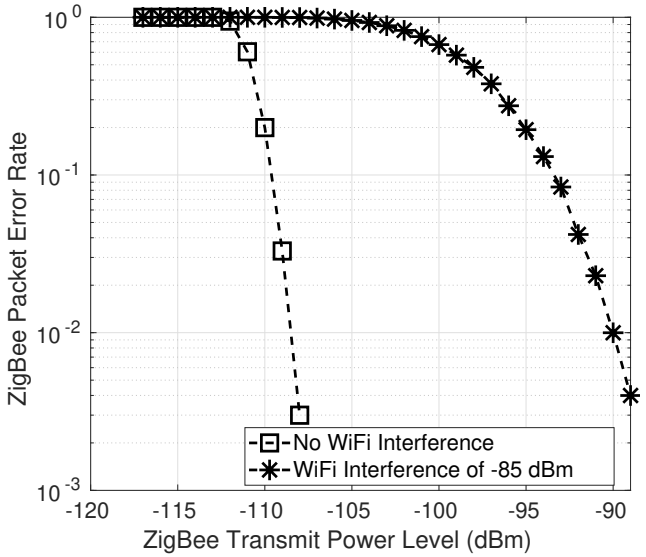


Fig. 4.9. PER of single antenna ZigBee receiver in the presence and absence of single antenna IEEE 802.11g transmitter(transmit power -85 dBm). Even at -85 dBm, which is lower than the minimum receiver sensitivity of IEEE 802.11g, ZigBee observes severe PER degradation.

physical layer signal processing methods to mitigate CCI for recovering both IEEE 802.11g and ZigBee on single and multi-antenna receivers.

4.2 Mitigating CCI in Single Antenna IEEE 802.11g Receiver Caused by ZigBee

In this section, we attempt to mitigate interference in single antenna IEEE 802.11g receiver caused by up to 4 single antenna ZigBee transmitters. We chose Soft Decision IEEE 802.11g receiver instead of Hard Decision Receiver because the former uses Soft Decision Viterbi Decoder (SDVD) which has proven to be robust compared to Hard Decision Viterbi Decoder (HDVD) in an interference-limited environment [60]. We start with a discussion on SDVD.

4.2.1 Soft Decision IEEE 802.11g Receiver and Noise Variance Estimation

After the incoming IEEE 802.11g frame has been detected and the frequency offset is corrected (using L-STF and L-LTF), the next tasks are estimating the channel, performing equalization and then decoding the data. The L-LTF symbol of the OFDM frame, as shown in Fig. 4.2 is used for channel and noise variance estimation. L-LTF consists of two identical OFDM symbols. After frame boundaries of the OFDM frame are detected (timing offset correction) and removal of cyclic prefix of every OFDM symbol, a N (N = 64 for IEEE 802.11g) point FFT of the OFDM frame is taken to obtain frequency domain samples which are written as:

$$Y(i,j) = X(i,j)H(i,j) + n(i,j), \quad 1 \leq i \leq N, \tag{4.1}$$

where $Y(i,j)$, $X(i,j)$ are complex samples representing received and sent symbols on the i-th subcarrier of the j-th OFDM symbol, respectively. Also, $H(i,j)$ is the channel transfer function of the i-th subcarrier for the j-th OFDM symbol. Term $n(i,j)$ contains components from both thermal noise, which is Gaussian and interference, which is not necessarily Gaussian. However, for this work, we model both noise sources as Gaussian with zero mean and variance $\sigma^2 = \{|n(i,j)|^2\}$. To estimate σ^2, L-LTF is used and the conventional way [76] of doing it is to perform an average over noise variances of all used subcarriers U_{sub} (52 for IEEE 802.11g [46]) in the L-LTF as follows:

$$\widehat{\sigma}^2 = \frac{1}{2U_{\text{sub}}} \sum_{i=1}^{U_{\text{sub}}} |Y(i,1) - Y(i,2)|^2, \tag{4.2}$$

where $Y(i,1)$, $Y(i,2)$ are the complex samples corresponding to i-th subcarrier of the first and second L-LTF symbols respectively. This $\widehat{\sigma}^2$ is used as noise variance for all the subcarriers of the OFDM data symbols following the L-LTF, i.e., SIGNAL and Payload field. The estimated noise variance is used to compute the approx Log Likelihood Ratios (LLRs) on per subcarrier basis [2]. The LLR $\Lambda(i,j,l)$ of the l-th bit corresponding to i-th subcarrier from j-th OFDM symbol is obtained as follows [80, Eq-2]:

$$\Lambda(i,j,l) = \frac{\min\limits_{z \in Z_0^l} \left(|Y(i,j) - H(i,j)z|^2 \right)}{\widehat{\sigma}^2} - \frac{\min\limits_{z \in Z_1^l} \left(|Y(i,j) - H(i,j)z|^2 \right)}{\widehat{\sigma}^2} \tag{4.3}$$

[2] In practice, the LLRs are approximated for efficiency and the approx LLRs [96],[80] are used in SDVD. From this point, we use the term LLR and approx LLR interchangeably.

where $Z_q^{(l)} = \{z|b_l(z) = q\}$ and b_l denotes the l-th bit in the gray mapping of z and $\widehat{\sigma}^2$ is the conventional noise variance estimate. We observe that the noise variance $\widehat{\sigma}^2$ acts as a scaling factor which scales the LLRs $\Lambda(i, j, l)$ according to the extent of noise variance on that subcarrier. A higher noise variance decreases the LLR while a smaller noise variance increases the LLR. We term the method of scaling the LLRs as in (4.3) as Conventional LLR Scaling (**Conv-SC**). In the absence of interference, the noise variance across the subcarriers is flat, i.e., AWGN. Thus, scaling all the LLRs using same noise variance estimate, i.e., Conv-SC works correctly. But, this is not the case in the presence of narrowband interference. Let's denote the set of all IEEE 802.11g subcarriers affected by ZigBee as S_{interf} and the set of rest of the subcarriers as $S_{\text{non-interf}}$. The S_{interf} may contain both pilot and data subcarriers. In the event of CCI, the noise variance on S_{interf} is higher compared to the noise variance on $S_{\text{non-interf}}$. Being the average noise variance over entire U_{sub}, $\widehat{\sigma}^2$ does not provide local noise variance (LNV)information across S_{interf}. Thus, the local estimation of noise power over S_{interf} and $S_{\text{non-interf}}$ is required in order to justify the scaling of $\Lambda(i, j, l)$.

4.2.2 Log-Likelihood Ratio Scaling with Localized Noise Variance of Interfered IEEE 802.11g Subcarriers (LNV-SC)

In this section, we discuss our work of [54] where we overcome the limitation of Conv-SC and propose modification to estimate local noise variance (LNV) estimates in the presence of single and multiple narrowband ZigBee interferers. Nonetheless, the method is equally applicable to any type of narrowband signal interfering wideband OFDM signal.

4.2.3 Localized Noise Variance Estimation

We start with a generalized case of K single antenna uncorrelated narrowband interferers (K single antenna ZigBee transmitters) and a single antenna IEEE 802.11g receiver. In our settings, S_k is the set of IEEE 802.11g subcarriers affected by the k-th ZigBee interferer ($k = 1, \ldots, K$) and S_0 is the set of all the subcarriers unaffected by any of the k interferers such that $S_0 \cup S_1 \cup .... \cup \ S_K = S_{\text{WiFi}}$, where$S_{\text{WiFi}}$ is the set of all IEEE 802.11g subcarriers. As the center frequencies of IEEE 802.11g and ZigBee in the 2.4 GHz band are fixed and their bandwidths are predefined, the knowledge of sets S_k and the set S_0 can be obtained apriori. An exemplary illustration for the case of 4 ZigBee interferers, centered at 2.430, 2.435, 2.440 and 2.445 GHz interfering a single IEEE 802.11g channel centered at 2.437 GHz is shown in Fig. 4.10. In this case $S_1 = \{1 \ldots 7\}$ and $S_2 = \{17 \ldots 23\}$, $S_3 = \{32 \ldots 38\}$, $S_4 = \{48 \ldots 52\}$ [3], $S_0 = S_{\text{WiFi}} – S_1 – S_2 – S_3 – S_4$. Thus, $|S_1| = |S_2| = |S_3| = |S_4| = 7$, $|S_0| = 24$ and $|S_{\text{WiFi}}| = U_{\text{sub}}$ where $|B|$ means the cardinality of the set B. For $k = 0, 1, \ldots, K$, we define the *LNV estimate* as follows:

$$\widehat{\sigma}^2_{S_k} = \frac{1}{2|S_k|} \sum_{i \in S_k} |Y(i, 1) - Y(i, 2)|^2. \tag{4.4}$$

We further define an index vector as

$$\left[\mathbf{V}_{S_k}\right]_i = \begin{cases} 1, i \in S_k \\ 0, i \notin S_k \end{cases} \qquad i = 1, 2, \ldots, U_{\text{sub}}. \tag{4.5}$$

[3]The last ZigBee channel affects only 5 subcarriers within the used subcarriers. Rest two affect subcarriers, i.e., 53 and 54 are unused

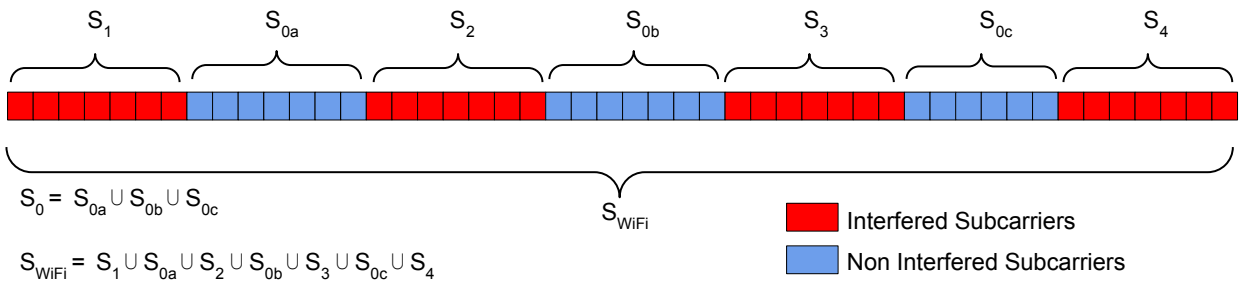


Fig. 4.10. Set of interfered and interference-free WiFi Subcarriers facing interference by 4 Co-Channel ZigBee Interferers

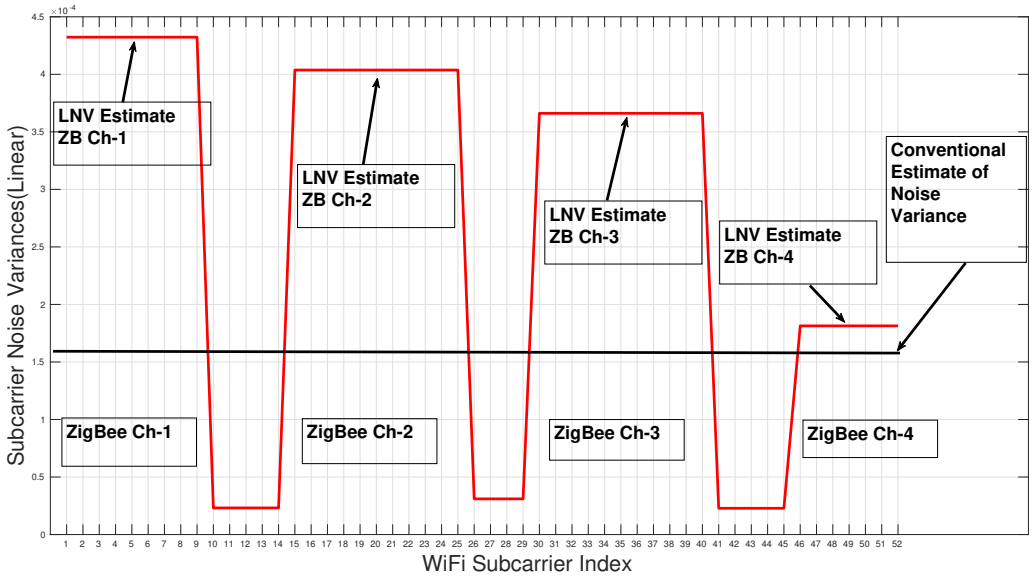


Fig. 4.11. LNV estimates corresponding to 4 ZigBee Interferers. Distinguish lobes appear at ZigBee center frequencies due to LNV estimation.

Using (4.4) and (4.5), we define a vector of noise variances over U_{sub} as:

$$\widehat{\boldsymbol{\sigma}}^2 = \sum_{k=0}^{K} \mathbf{V}_{S_k} \widehat{\sigma}^2_{S_k}, \tag{4.6}$$

Corresponding to Fig. 4.10, the plot of vector of noise variances $\widehat{\boldsymbol{\sigma}}^2$ for 4 ZigBee interferers to a single WiFi channel is shown in Fig. 4.11. In the same figure, we also plot the noise variance obtained conventionally, i.e., $\widehat{\sigma}^2$ shown by a flat black line as it is constant over the entire span of used subcarriers. In contrast, the plot of LNV vector, i.e., $\widehat{\boldsymbol{\sigma}}^2$, produce distinguishably elevated lobes centered on the corresponding ZigBee center frequencies. Such lobes give information about two important things:

- The presence of interferers
- The excess noise variance induced by the interferers

Finally using (4.4), (4.5) and (4.6), we can modify (4.3) to obtain the scaled LLRs as

$$\Lambda(i,j,l) = \frac{\min\limits_{z \in Z_0^l} \left(|y(i,j) - H(i,j)z|^2 \right)}{\widehat{\sigma_i}^2} - \frac{\min\limits_{z \in Z_1^l} \left(|y(i,j) - H(i,j)z|^2 \right)}{\widehat{\sigma_i}^2} \tag{4.7}$$

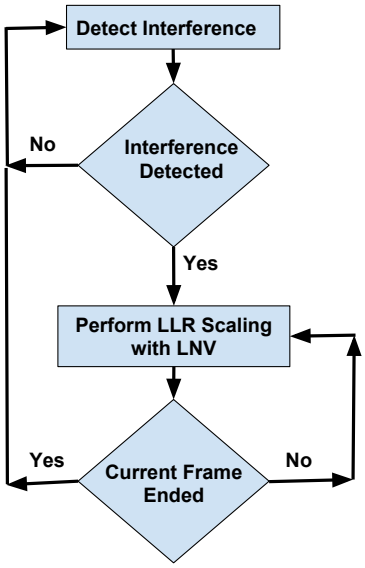


Fig. 4.12. Flow Chart of Interference Detection and LLR Scaling. LLR scaling using LNV (LNV-SC) to be performed only during interference.

where $\widehat{\sigma_i}^2$ is the i-th element of the vector $\widehat{\boldsymbol{\sigma}}^2$ and $i = 1, 2, \ldots, U_{\text{sub}}$. We term our method of LLR scaling using LNV estimates as **LNV-SC**. The LLRs are further sent to SDVD for the rest of the processing steps.

To initiate the process of **LNV-SC**, the IEEE 802.11g receiver needs to know the presence or appearance of single or multiple ZigBee interferers. In the next section, we discuss our method of interference detection [54] which is a by-product of the computation of LNV-SC.

4.2.4 Multiple Narrowband Interference Detection

From Fig. 4.11, it is observed that for K number of interferers, the vector of noise variances $\widehat{\boldsymbol{\sigma}}^2$ observes sharp and distinguish rise in magnitude over the regions where the narrowband signals are present compared to the regions unaffected by narrowband signals. For a given IEEE 802.11g channel, the overlapping ZigBee channels center frequencies are known a priori from the frequency allocation also shown in Fig. 4.6. Thus the elevated portions in Fig. 4.11 give a coarse estimate of the presence of the interferers. This knowledge is combined along with a threshold detector to pinpoint the interferers as soon as they appear. In practice, the LNV is estimated at all the possible center frequencies of the interferer. Upon detecting the presence of interferers, the corresponding LNV is used to scale the LLRs. The entire operation of interference detection and LLR scaling is illustrated in Fig. 4.12.

Our proposed method of interference detection does not add any additional signal processing complexity as it is a byproduct of LNV-SC. The key advantage of our approach is that lobes could be obtained even at the shallow level of interference. However, the method is effective only when there is an overlap between L-LTF of IEEE 802.11g and an ongoing ZigBee transmission as the method uses L-LTF (duration 0.8 µs) to calculate $\widehat{\sigma}^2$. This is a fair assumption as the typical frame lengths of IEEE 802.11g (194 µs − 542 µs) are shorter than that of ZigBee (352 µs − 4256 µs) [62]. To detect the appearance of ZigBee interference during an ongoing IEEE 802.11g transmission, i.e., when L-LTF is not interfered, pilot subcarriers embedded under every OFDM data symbols of IEEE 802.11g could be used however the estimation accuracy could be affected as there are only 4 pilots subcarriers within 48 data subcarriers.

Table 4.1: Simulation Parameters

Channel Model WiFi	11 tap Rayleigh, Exponential Power Delay profile, RMS Delay Spread 49 ns
Channel Model ZigBee	1 tap Rayleigh
Noise Power	−100 dBm
IEEE 802.11g PSDU	1000 bytes
ZigBee PSDU	120 bytes
Sampling Rate	WiFi 20 MHz, ZigBee oversampled to 20 MHz

Table 4.2: Transmit Power Gain(dB) of LNV-SC compared to Conv-SC

WiFi MCS / # of Interferers	0	2	4	6
1	3.9	3.5	3.8	3.8
2	3	3	2.9	2.7
4	1.5	1.5	1.5	1.2

4.2.5 Simulations and Results

To validate our methods LNV-Sc and interference detection, we perform Monte Carlo simulations using the standard compliant IEEE 802.11g and IEEE 802.15.4 libraries available in release 2017b of MATLAB. We simulated the worst case scenario, i.e., when lack of CSMA/CA creates a 100% chance of collision. The simulation parameters are mentioned in Table 4.1. For all the experiments, we choose Transmit Power level (TxP) required to achieve 10% PER as our performance metric[4]. We simulate the entire RF front-end which includes simulating the behavior of frame synchronization and timing synchronization in the presence of interference.

4.2.5.1 Comparing LNV-SC and Conv-SC

To compare LNV-SC and Conv-SC, we simulate interference between single IEEE 802.11g channel and up to 4 ZigBee channels. TxP of ZigBee channels are fixed to −85 dBm which is the minimum TxP required(in 2.4 GHz band) to achieve 1% PER [41], while IEEE 802.11g TxP is varied to achieve $< 10\%$ PER. We present results for IEEE 802.11g MCS 0 (BPSK) and MCS 2 (QPSK) in in Fig. 4.13 and Fig. 4.14 respectively. We observe that with LNV-SC, the 10% PER mark is reached at a lower TxP compared to Conv-SC. We term the difference in TxP observed between LNV-SC and Conv-SC as *Transmit Power Gain*(TPG) which is summarized in Table 4.2 for MCS $0, 2, 4$ and 6. From Table 4.2 we observe the following:

- As the number of ZigBee channels increases, TPG monotonically decreases because more IEEE 802.11g OFDM subcarriers get affected which decreases the difference between noise variance estimates calculated using Conv-SC and LNV-SC.

- TPG is consistent throughout the MCS for a given number of interferers. This is due to the fixed payload size of IEEE 802.11g (1000 bytes) which we used for simulations leading to an equal number of LLRs getting affected in all the MCS.

[4]This performance metrics criterion is mentioned in [46, Sec-17.3.10.4].

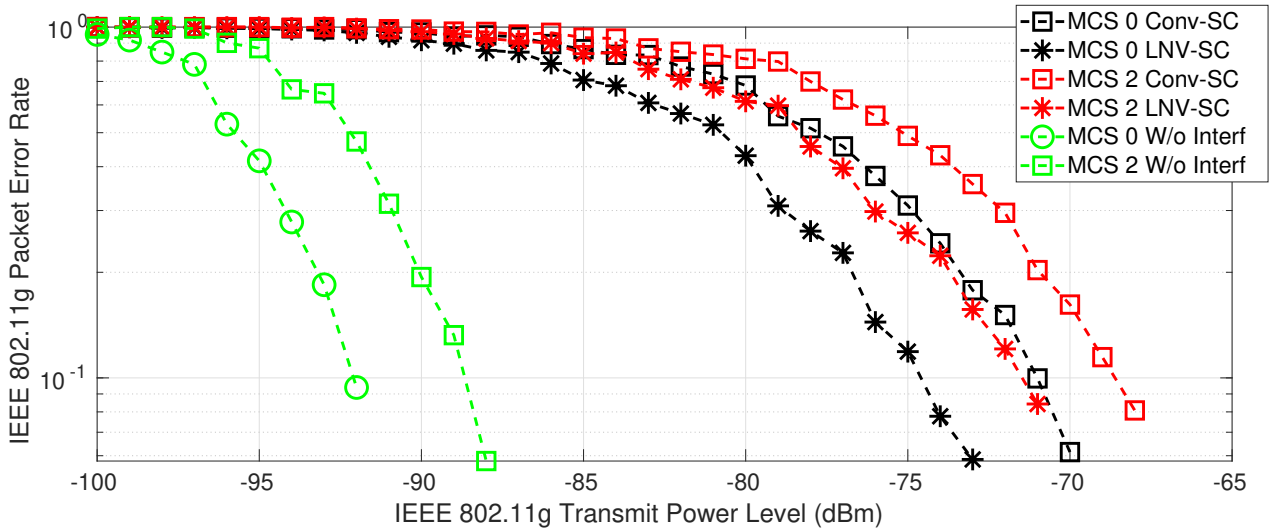


Fig. 4.13. Performance of LNV-SC for IEEE 802.11g MCS 0 and 2 facing interference from single ZigBee channel at −85 dBm. LNV-SC observes an average transmit power gain of 3.7 dB over Conv-SC for all the MCS.

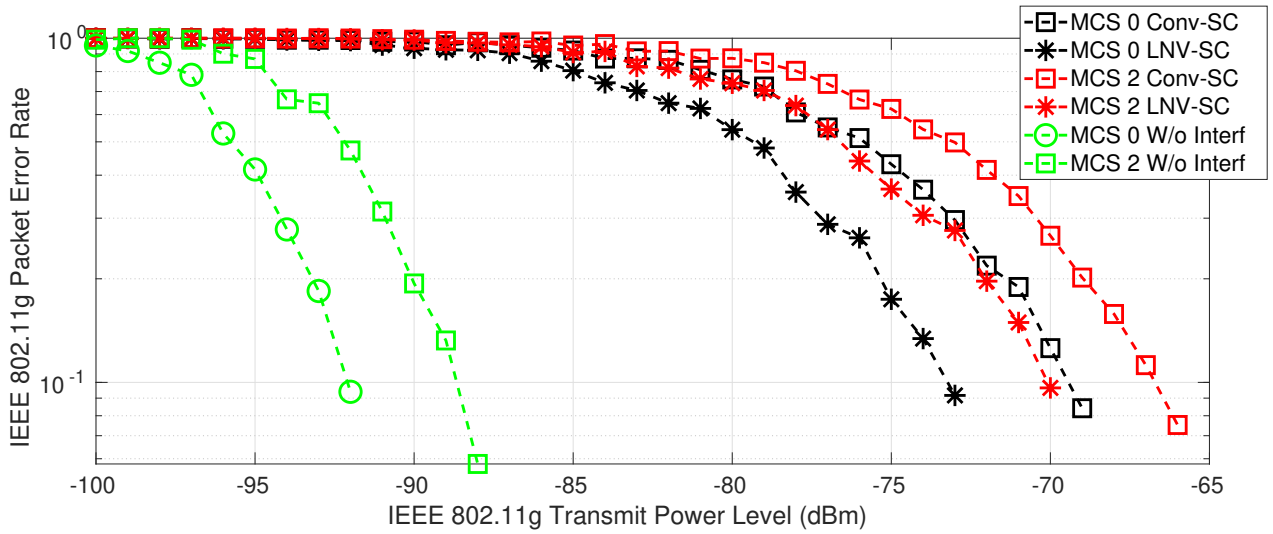


Fig. 4.14. Performance of LNV-SC for IEEE 802.11g MCS 0 and 2 facing interference from two ZigBee channels at −85 dBm. LNV-SC observes an average transmit power gain of 3 dB over Conv-SC for all the MCS.

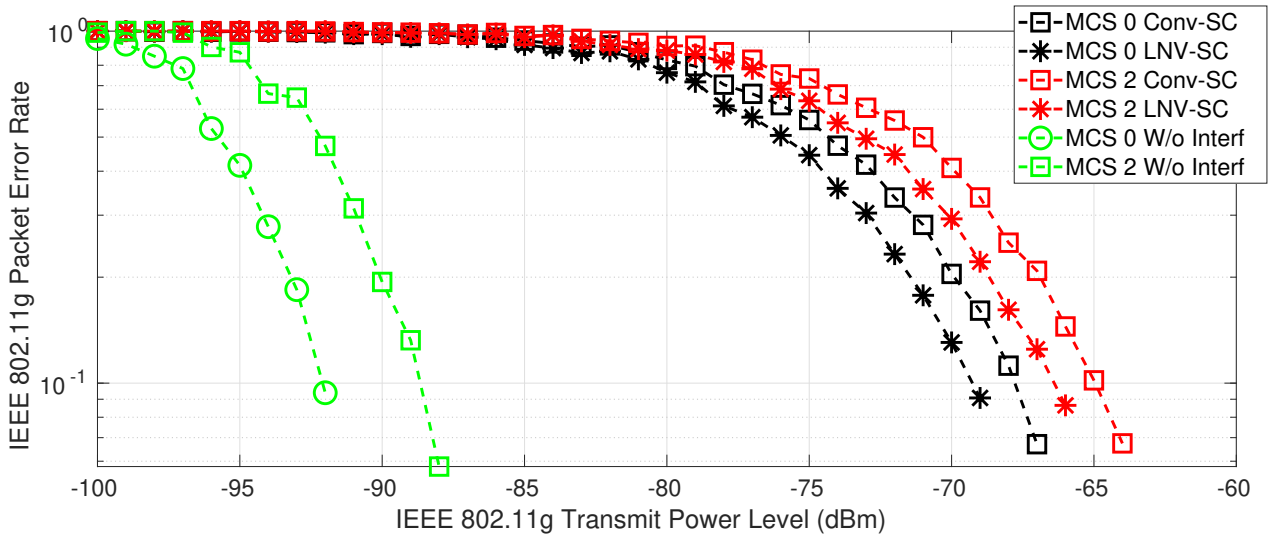


Fig. 4.15. Performance of LNV-SC for IEEE 802.11g MCS 0 and 2 facing interference from four ZigBee channels at −85 dBm. LNV-SC observes an average transmit power gain of 1.5 dB over Conv-SC for all the MCS.

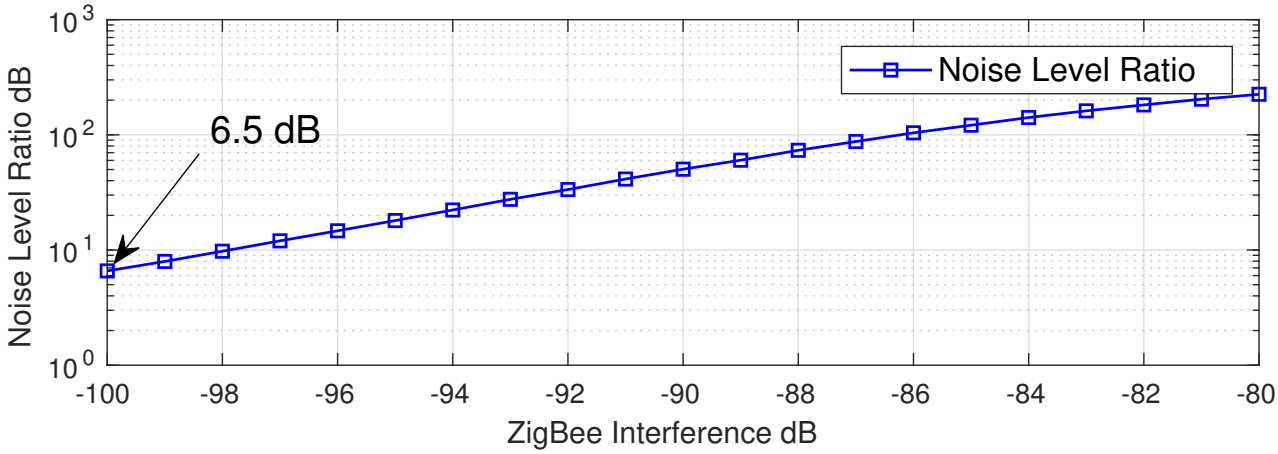


Fig. 4.16. Noise Level Ratio: Ratio of the LNV of the interfered region to that of the region without interference for fixed WiFi TXP -80 dBm. Even at low interference TxP of -100 dBm, the NLR is 6.5 dB which is sufficient to detect the presence of interference.

4.2.5.2 Interference Detection

To test our method of interference detection, we calculate the ratio of the LNV of the interfered region to that of the region without interference for a fixed WiFi TxP (−80 dBm) and varying TxP of a single ZigBee channel from −100 dBm to −80 dBm. We term this ratio as *Noise Level Ratio* (**NLR**). In the geometrical representation, the level of NLR defines the height of lobes relative to the noise floor as illustrated in Fig. 4.11. The more prominent the lobe is, the more accurate is its detection using a threshold detector. From Fig. 4.16, we observe that even at low interference TxP (−100 dBm), the NLR is 6.5 dB which is sufficient to detect the presence of interference.

4.2.6 Discussion

A positive TPG for LNV-SC indicates that for a given IEEE 802.11g TxP, LNV-SC can achieve lesser PER compared to Conv-SC. Lesser PER means more packets could be recovered in the event of interference with ZigBee which fulfills the motive of SMS-SDR. However, LNV-SC is only capable of recovering the packets which have already been detected. In other words SINR of IEEE 802.11g has

to be sufficient enough to be detected at the receiver, i.e., Frame Synchronization. In addition, due to interference, the timing offset estimation could also be affected leading to wrong output of FFT operation. Thus, if frame synchronization and timing offset detection fails; unfortunately the frame cannot be recovered with LNV-SC. Nonetheless, LNV-SC is very simple to implement in the existing IEEE 802.11g receivers as well as any wireless standard which uses OFDM for their PHY.

The efficiency of the NLR based interference detection method will depend upon the threshold which will vary from one setting to another; hence an initial training and calibration will be required. Nonetheless, NLR based method to detect the interference is a by-product of LNV-SC, i.e., no additional signal processing is required. On the down side, NLR can detect only narrowband interferers. For wideband interferers, other methods such as Error Vector Magnitude (EVM) between decoded and regenerated samples of the stronger signal can be used [56].

4.2.7 Limitations of LLR Scaling based Methods for OFDM Systems

Although LNV-SC provides significant gain while recovering interfered IEEE 802.11g packets, following two cases could be argued where LNV-SC could malfunction:

- **Case-1**: LNV-SC requires IEEE 802.11g to be strong enough so that at least the frame synchronization is successful in the event of collision. L-STF, which form the very beginning of a IEEE 802.11g frame are responsible for frame synchronization. L-STF are BPSK modulated to have robustness, nonetheless, a high powered nearby ZigBee transmitter can destroy the structure of L-STF leaving the entire IEEE 802.11g frame non-detectable.

- **Case-2**: If ZigBee frame corrupts an IEEE 802.11g frame in such a manner that L-STF and L-LTF are not interfered, but SIGNAL field and payload are affected. In such case, the interference cannot not be detected as discussed in Section 4.2.4. In the absence of interference detection, LNV-SC will not function.

In the next section, we discuss methods which overcome the limitations of LNV-SC.

4.2.8 Successive Interference Cancellation of ZigBee from IEEE 802.11g

Successive Interference Cancellation is a well known physical layer technique to recover a weaker signal corrupted by a stronger signal [71]. Let $s^z[n]$ and $s^w[n]$ be the time domain ZigBee and IEEE 802.11g signals respectively. In the event of collision, the composite signal $r[n]$ can be written as:

$$r[n] = h^w[n] * s^w[n] + h^z[n] * s^z[n] + v[n] \tag{4.8}$$

where h^w and h^z are time domain impulse responses of IEEE 802.11g and ZigBee channels respectively. Term $v[n]$ represents Gaussian distributed thermal noise samples with zero mean and variance σ^2. Note that since the sampling rates of IEEE 802.11g (20 MHz) and ZigBee (2 MHz) are different, an appropriate resampling needs to be performed before realizing (4.8). Without loosing the generality, lets consider IEEE 802.11g as our SOI, the Signal to Interference plus Noise Ratio (SINR) of IEEE 802.11g in the received signal $r[n]$ is

$$\mathrm{SINR}_{\mathrm{WF}}[n] = \frac{\mathbb{E}\{|h^w[n] * s^w[n]|^2\}}{\mathbb{E}\{|h^z[n] * s^z[n]|^2\} + \sigma^2}. \tag{4.9}$$

With this SINR_{WF}, the detection and decoding of a IEEE 802.11g frame depend on the strength of the ZigBee interference. In order to increase SINR_{WF}, SIC can be applied over $r[n]$. SIC is possible when the receiver can decode the stronger signal and cancel its effect from the composite signal. By performing SIC, the effective post-processing SINR of the weaker signal is likely to exceed the required receiver sensitivity [71] of the weaker signal. A power difference of 5-20 dBm is required for an efficient operation of SIC [101]. It is possible to have such power difference when a strong ZigBee transmitter is located nearby the IEEE 802.11g receiver.

The process of SIC starts when a strong ZigBee signal is detected and decoded at the receiver. During the process of decoding, the channel estimates of ZigBee are stored, and once the decoded bits are available, the channel estimates are used to regenerate the ZigBee signal back. In the next section we first, discuss the channel estimation process for a detected ZigBee frame.

4.2.9 Channel Estimation for ZigBee

ZigBee employs direct sequence spread spectrum (DSSS) that uses a digital spreading function representing pseudorandom noise (PN) chip sequences [41], [83]. The radio encodes these chip sequences using orthogonal quadrature phase shift keying (O-QPSK) and transmits them at 2 Mchips/s or 250 Kbps. Thus the duration of one bit is $1/250000 = 4$us. Maximum delay spread in 2.4GHz is of the order of nano seconds [94] which is significantly less than the bit period of ZigBee which is 4us. This indicates that in most of the environments, a ZigBee signal will experience frequency flat fading, i.e, single tap channel in the time domain. However, unlike IEEE 802.11g, ZigBee does not have pilots to estimate the channel. Nonetheless, the preamble structure of ZigBee as shown in Fig. 4.4 provides an intuitive way of doing so. As shown in Fig. 4.4, the ZigBee frame is preceded by a *Preamble* and *Start of Frame Delimiter* (SFD), jointly called Synchronization Header (SHR). Preamble consists of 4 byte, all set to 0 and SFD is 1 byte long with the value set to 0X7A. SHR is used at the receiver to detect the incoming ZigBee frame, i.e., frame synchronization pin point the frame boundary. We use the known symbols corresponding to SHR to estimate the single tap ZigBee channel. Consider the transmitted vector $\overline{S}^z$ and received vector $\overline{Y}^z$ corresponding to the known SHR samples as follows:

$$\overline{Y}^z = h^z * \overline{S}^z + \overline{V}, \tag{4.10}$$

where h^z is the single tap channel, $\overline{V}$ is the noise vector. Each of the vectors in (4.10) are $NX1$ dimensional where N is the total number of samples corresponding to SHR. [5]. The Maximum Likelihood estimate of h^z can be written as:

$$\hat{h}^z = \frac{(\overline{S}^z)^{\text{T}}\overline{Y}^z}{(\overline{S}^z)^{\text{T}}\overline{S}^z} \tag{4.11}$$

Method as in (4.11) can be used to estimate the ZigBee channel only when it is single tap; nonetheless, as discussed, indoor channel for ZigBee in 2.4 GHz is mostly single tap. For multi-tap ZigBee channel, the method discussed in [59] can be used. Once the channel of ZigBee is estimated, next, we regenerate the estimate of time domain ZigBee signal as follows:

$$y^z_{\text{Reg}}[n] = \hat{h}^z[n] * s^z[n]. \tag{4.12}$$

[5] In practice, many samples of Preambles are lost before the frame is detected, hence, samples corresponding to the SFD can be used for estimating the channel; however, the sampling accuracy may be affected

Note that we use only those ZigBee frames for regeneration which have passed the CRC test. After that SIC is performed by subtracting the regenerated signal from the received signal:

$$y_{\text{SIC}}[n] = h^w[n] * s^w[n] + (h^z[n] - \hat{h}^z[n]) * s^z[n] + v[n]. \tag{4.13}$$

After SIC, the post processing SINR of weaker WiFi becomes:

$$\text{SINR}_{\text{WF}}^{\text{SIC}}[n] = \frac{\mathbb{E}\{|h^w[n] * s^w[n]|^2\}}{\mathbb{E}\{|(h^z[n] - \hat{h}^z[n]) * s^z[n]|^2\} + \sigma^2}. \tag{4.14}$$

From (4.14), it can be observed that the more accurate is the channel estimate $\hat{h}^z$, the smaller is the noise term $\mathbb{E}\{|(h^z - \hat{h}^z) * s^z|^2\} + \hat{\sigma}^2$ in the denominator and the higher is post processing SINR of IEEE 802.11g. With this post processing SINR, it is possible to detect the IEEE 802.11g frames in the residue signal, i.e., $y_{\text{SIC}}[n]$ by performing the frame synchronization routines.

4.2.10 Simulations and Results

To validate the performance of SIC, we perform Monte Carlo simulations using the standard compliant IEEE 802.11g and IEEE 802.15.4 libraries available in release 2017b of MATLAB. Interference is caused by a single channel single antenna ZigBee transmitter whose TxP is fixed to -60 dBm. We performed simulations for IEEE 802.11g MCS 2 and 4. Simulation parameters are the same as mentioned in Table 4.1. We log Packet Error Rate (PER) and Synchronization Error Rate (SER) as our performance metric. We first plot the SER for IEEE 802.11g MCS 2 and 4 in Fig. 4.17. We observe that high powered ZigBee severely affects the frame synchronization of IEEE 802.11g frames, i.e., IEEE 802.11g frames not being detected at all. Although performing SIC provides advantage over no SIC, the overall SER stays very high. We also observe that SER for both IEEE MCS 0 and 2 are almost the same. This is explained by the fact that regardless of the MCS of IEEE 802.11g, the preambles (L-STF and L-LTF) are always modulated using BPSK. Next we plot the PER for IEEE MCS 0 and 2 in Fig. 4.18 and Fig. 4.19 respectively. We observe the following from PER plots:

- Presence of high power ZigBee severely degrades the PER of IEEE 802.11g. The degradation is caused by synchronization error as well as CRC error.
- Performing SIC provides advantage over not performing SIC. This is observed over a region of SNR which is highlighted by green rectangle in both the plots.
- The gain observed due to SIC fades away as the MCS increases. This can be explained by the fact that at higher MCS, i.e., higher QAM constellations, the SINR requirement is also high which may not be obtained by SIC.

4.2.11 Discussion

SIC overcomes the limitations of LNV-SC and MLSC. Nonetheless LLR scaling can again be applied over the weaker signal for possible improvement in PER. A distinguish advantage of SIC is the capability of resynchronization of the weaker signal, i.e., frame detection of weaker signal which is otherwise undetectable due to interference. Although, we experimented for single ZigBee channel, but the method can be extended for the case of multiple ZigBee channels too. Another significant advantage of SIC is that it can be used for signals which have comparable bandwidth, which is

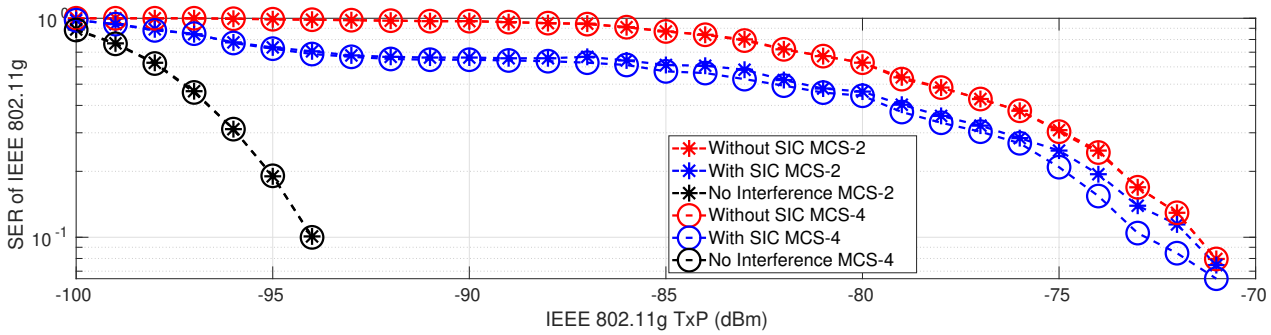


Fig. 4.17. Synchronization Error Rate (SER) of IEEE 802.11g MCS 2 and 4 after SIC of ZigBee (−80 dBm). SER for both MCS is similar as the preamble of IEEE 802.11g is BPSK mobulated regardless of the MCS

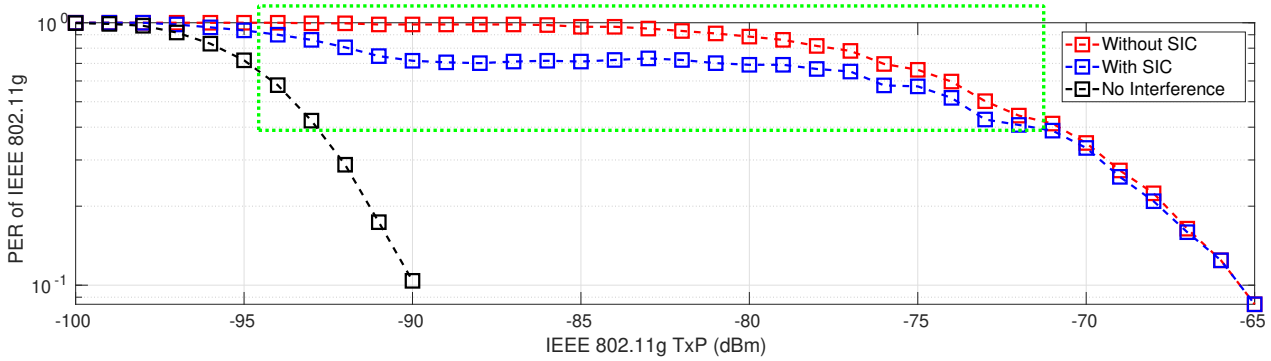


Fig. 4.18. Packet Error Rate of IEEE 802.11g, MCS 2 after SIC of ZigBee (−80 dBm). Region over which SIC provides gain is highlighted in green rectangle.

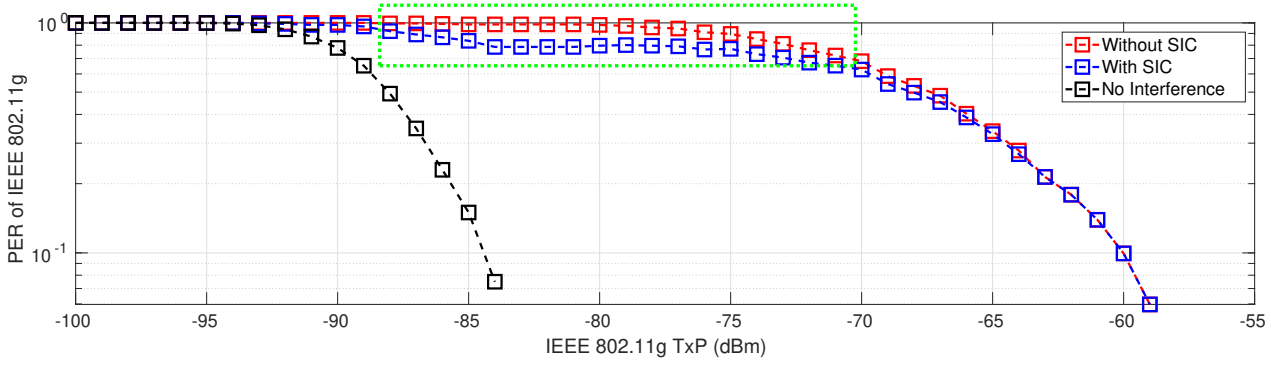


Fig. 4.19. Packet Error Rate of IEEE 802.11g, MCS 4 after SIC of ZigBee (−80 dBm). Region over which SIC provides gain is highlighted in green rectangle.

in contrast to LLR scaling based methods. However the benefits of SIC fade away as the QAM constellations gets dense. Also, the performance of SIC majorly depends on the accurate regeneration of the stronger signal which in turn depends on the accuracy of channel estimates. In the event of interference, channel estimates accuracy, even for the stronger signal, is affected. In next sections and chapters, we propose methods to overcome these limitations of SIC.

4.3 Testing LNV-SC for its General Applicability

With the discussion of SIC, our development of interference mitigation methods for single antenna wideband OFDM receivers is finished. Before we proceed to multi-antenna receivers, we briefly test LNV-SC for its generalized applicability to other wireless signals. We choose IEEE 802.11ax [37], [23] as the wideband OFDM signal and another signal which is based on SC-FDMA [43] as the narrowband signal. We start with a discussion on physical layer of both the signals followed by implementation of LNV-SC to recover wideband IEEE 802.11ax from narrowband SC-FDMA interference.

4.4 Physical Layer of 802.11ax and SC-FDMA

IEEE 802.11ax is the upcoming generation in the IEEE 802.11 family with a scheduled release in 2019 end. It is also known as WiFi-6 and can achieve throughput upto 10 Gbps. It comes under High Efficiency (HE) category with major changes in its physical layer. It will be operational in both 2.4 GHz and 5 GHz unlicensed band. SC-FDMA is not a wireless standard but a physical layer used by LTE for its uplink in order to get more power efficiency. With the proposals by 3GPP to let LTE enter in the unlicensed bands, termed as LTE Licensed Assisted Access(LTE-LAA), the interference between IEEE 802.11ax and LTE-LAA is inevitable. We start our discussion with the physical layer of IEEE 802.11ax and SC-FDMA in brief.

4.4.1 Physical Layer of 802.11ax

We choose IEEE 802.11ax as it is a wideband OFDM signal having physical layer different from previous IEEE 802.11 wireless standards. In contrast to IEEE 802.11n and IEEE 802.11ac which primarily focus on high throughputs, IEEE 802.11ax focuses on efficiency. Some of the major advancements in IEEE 802.11ax include:

- 256 point FFT compared to 64 point FFT in IEEE 802.11a/g/n/ac. Higher FFT point gives more number of subcarriers within the same bandwidth of 20 MHz.
- OFDMA support in both uplink and downlink to enable multiuser support.
- LTE type resource allocation enables QoS for various users and services.
- Support for higher QAM such as 1024. This enables the gigantic achievable throughput of up to 10 Gbps.
- 4x larger OFDM symbol duration provides improved robustness to outdoor environment characterized by large delay spreads.

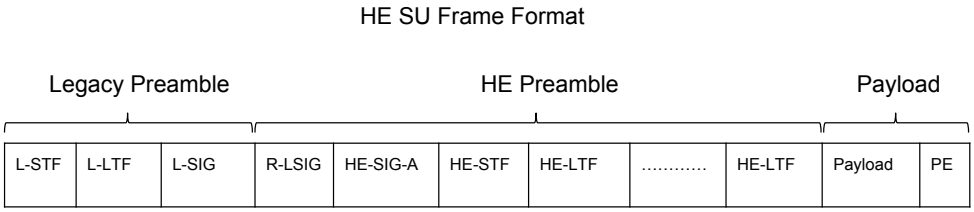


Fig. 4.20. Single user frame format of IEEE 802.11ax

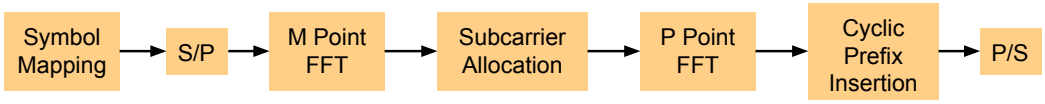


Fig. 4.21. A block diagram of SC-FDMA

A typical frame format for IEEE 802.11ax single user is shown in Fig. 4.20. We can see that the frame consists of Legacy IEEE 802.11 Preambles also. Among the HE preamble, the HE-STF training field is used for timing synchronization while the HE-LTF is used for channel estimation, enabling beamforming and MIMO spatial diversity. 256 point FFT in IEEE 802.11ax results in 256 subcarriers with a spacing of 78.125 KHz. Out of total 256 subcarriers, 234 are used as data subcarriers, 8 are used as pilot subcarriers, 3 subcarriers at the center are left as DC and 11 subcarriers are unused.

4.4.2 SC-FDMA

SC-FDMA is a modulation scheme used by LTE-LAA uplink as it provides significantly lower Peak to Average Power Ratio (PAPR) compared to OFDM [72]. Likewise OFDM, SC-FDMA also produces orthogonal subcarriers. A block diagram of SC-FDMA transmitter is shown in Fig. 4.21. The significant difference between SC-FDMA and OFDM transmitter is the insertion of an extra FFT block before the IFFT block. Performing FFT before IFFT spreads the power evenly among subcarriers reducing the PAPR [72]. In LTE-LAA, the resource allocation is performed in the units of *Resource Blocks* where each resource block consists of 12 SC-FDMA subcarriers. By selecting appropriate number of resource blocks and sampling rates, the bandwidth of SC-FDMA can be varied. Section 4.4.2 shows the relation between number of resource blocks and the bandwidth in SC-FDMA signal.

4.4.3 Mitigating CCI in Single-antenna IEEE 802.11ax Receiver Caused by SC-FDMA

We consider a scenario where a single antenna 20 MHz IEEE 802.11ax receiver is facing interference from another single antenna SC-FDMA transmitter. We configure SC-FDMA for 3 MHz and 5 MHz

Table 4.3: SC-FDMA specifications used in LTE Uplink (20 MHz)

Channel Bandwidth (MHz)	20
Number of Resource Blocks	100
Number of Occupied Subcarriers	1200
IFFT/FFT (P in Fig. 4.21)	2048
Sample Rate (MHz)	30.72

Table 4.4: Simulation parameters for interference between IEEE 802.11ax and SC-FDMA

	IEEE 802.11ax	SC-FDMA
MCS	0 (BPSK)	BPSK
Noise Power	-100 dBm	
Bandwidth (MHz)	20	3, 5
Sampling Rate (MHz)	20	3.84, 7.68
Channel Model	TGax channel, Model-A	Extended Pedestrian Channel Model-A

bandwidth by generating the waveform with 15 and 25 resource blocks respectively. This is the case of interference between wideband OFDM signal and narrowband signal. Now we attempt to recover IEEE 802.11ax signal by applying LNV-SC.

4.4.4 Applying LNV-SC to IEEE 802.11ax

LNV-SC requires computation of LNV estimates, however, the computation of LNV estimates in a standard IEEE 802.11ax receiver posses some challenges. Out of total 256 subcarriers, only 8 subcarriers are used as pilot subcarriers for noise variance estimation. Thus they are not sufficient for noise variance estimation per subcarrier as the spacing between the pilot subcarriers is large. Although, L-LTF from the legacy preamble has 52 used subcarriers, 312.5 KHz wide each and IEEE 802.11ax payloads have 242 used subcarriers (pilot + data), 78.125 KHz wide each, both L-LTF and payload occupy same bandwidth (in our case 20 MHz). Thus we propose to estimate the LNV using L-LTF and map them over the payload subcarriers to span the entire used bandwidth of IEEE 802.11ax.

4.4.5 Simulations and Results

To validate the performance of LNV-SC over Conv-SC in recovering IEEE 802.11ax facing interference from SC-FDMA signal, we created interference between single antenna single channel 20 MHz IEEE 802.11ax at MCS 0 (BPSK) and $3, 5$ MHz SC-FDMA signals. Transmit power of SC-FDMA signal is kept constant at -85 dBm. We perform Monte Carlo simulations using the standard compliant IEEE 802.11ax and SC-FDMA libraries available in release 2018a of MATLAB. We created the worst case scenario as if there is not CSMA/CA making 100% chances of collision. Simulation parameters are summarized in Section 4.4.4. We choose Transmit Power level (TxP) required to achieve 10% PER as our performance metric for the experiments. PER plot for the case interference from 3 MHz and 5 MHz are shown in Fig. 4.22 and Fig. 4.23 respectively. From the plots we observe the following:

- Presence of SC-FDMA signal degrades the performance of IEEE 802.11ax. The degradation increases with increase in the bandwidth of SC-FDMA signal as more number of subcarriers of IEEE 802.11ax are affected. Quantitatively, since the subcarrier width of IEEE 802.11ax is 78.125 KHz, the number of affected subcarriers by 3 and 5 MHz SC-FDMA is approximately 39 and 64 respectively.

- Applying LNV-SC provides significant transmit power gain over Conv-SC. This is seen for both 3 MHz (6 dB of gain) and 5 MHz (5 dB of gain)SC-FDMA. As expected, the gain decreases from 3 MHz to 5 MHz.

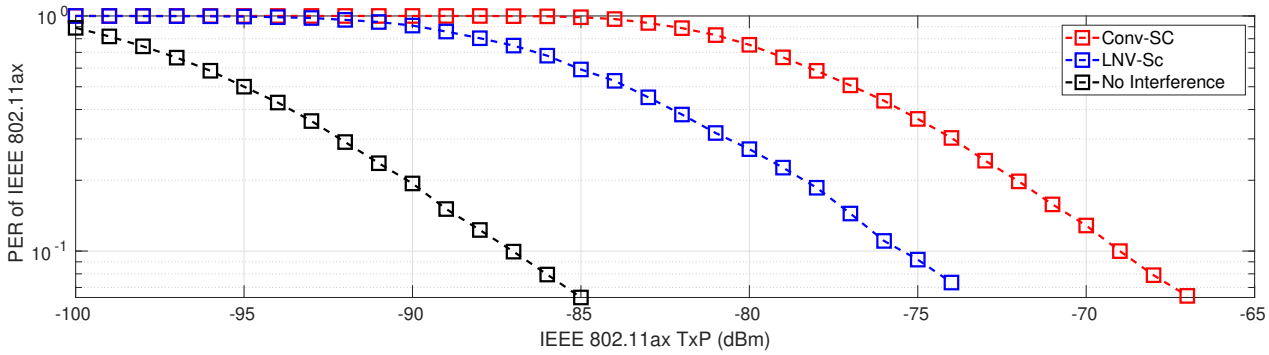


Fig. 4.22. Comparison of LNV-SC and Conv-SC in improving PER of IEEE 802.11ax MCS 0 facing interference from 3 MHz SC-FDMA (−85 dBm) signal. LNV-SC performs better than Conv-SC

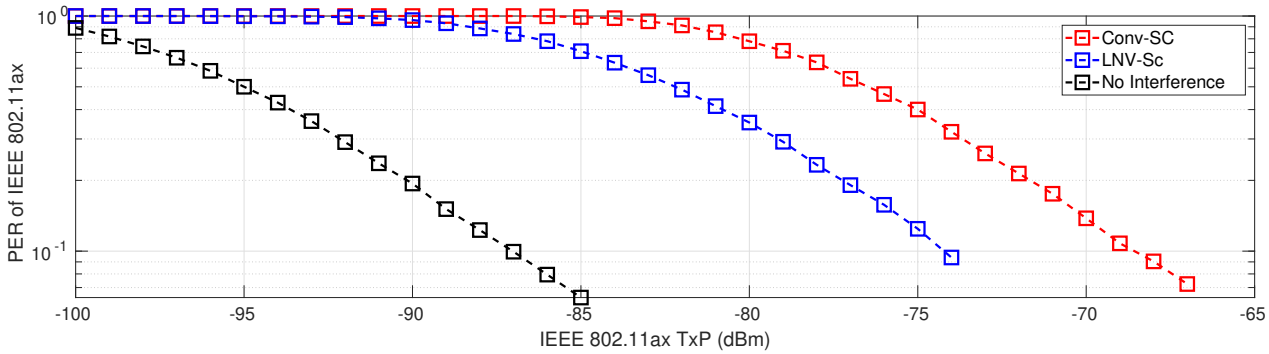


Fig. 4.23. Comparison of LNV-SC and Conv-SC in improving PER of IEEE 802.11ax MCS 0 facing interference from 5 MHz SC-FDMA (−85 dBm) signal. LNV-SC performs better than Conv-SC

4.4.6 Discussion

In Section 4.2.2, through simulations, we show the effectiveness of LNV-SC in recovering wideband OFDM IEEE 802.11g facing interference from narrowband ZigBee signals. In this section, we applied the same method for a similar case of wideband OFDM and narrowband signals and observed similar results where LNV-SC outperforming Conv-SC. These experiments prove the generality of LNV-SC.

4.5 Mitigating CCI in Multi-antenna IEEE 802.11g Receiver Caused by ZigBee

Diversity is a well-known concept of combating the effects of multipath fading [90]. In particular, we talk about spatial diversity which uses multiple antennas to extract uncorrelated fading signals. By using omni-directional antennas and neglecting the effects of coupling between antennas, the observations of signals on the multiple antennas would be uncorrelated if observed 0.38λ apart. The underlying mechanism providing diversity gain is the decreasing probability of simultaneous deep fades on all the antenna branches with an increasing number of antenna branches [33]. An additional benefit of diversity is that likewise the desired signal, the interference also travels through different paths, and if the path followed by interference corresponding to one antenna is in deep fade, it is beneficial for the desired signal on that particular antenna! In this section, we attempt to leverage this phenomena and extend our previous method **LNV-SC** for multi-antenna IEEE 802.11g receiver. We consider the automated industries and smart homes where IEEE 802.11g and ZigBee nodes are generously used; such environments are also characterized by rich multi-paths[19].

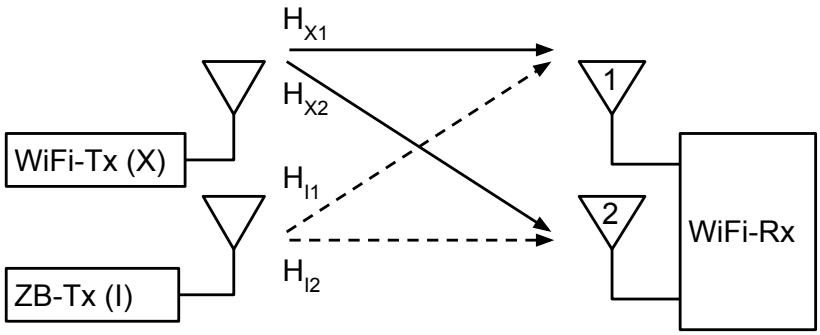


Fig. 4.24. Signal Model: Single Antenna IEEE 802.11g Transmitter, Single Antenna ZigBee Interferer and Two Antenna IEEE 802.11g receiver

In the following, we discuss our work [55] which is a multi-antenna extension to LNV-SC. We start our discussion with the popular diversity combining method Maximal Ratio Combiner followed by legacy CCI mitigation method Optimal Combiner and state-of-the art CCI mitigation technique Technology Independent MIMO (TIMO) [34]; but first we develop the multi-antenna signal model.

4.5.1 Multi-Antenna Signal Model

The signal model consists of a dual-antenna IEEE 802.11g receiver (WiFi-Rx), a single antenna IEEE 802.11g transmitter (WiFi-Tx), and a single antenna ZigBee transmitter (ZB-Tx) as illustrated in Fig. 4.24. As IEEE 802.11g is our Signal of Interest (SOI), we assume that after collision, the IEEE 802.11g signal is strong enough to pass frame synchronization. After the correct timing offset detection a 64 FFT is performed and the received signal vector $\mathbf{Y}$ on i-th subcarrier of j-th IEEE 802.11g OFDM symbol with the desired IEEE 802.11g and interfering ZigBee samples $X(i,j)$ and $I(i,j)$ respectively can be written as:

$$\mathbf{Y}(i,j) = X(i,j)\mathbf{H}_X(i) + I(i,j)\mathbf{H}_I(i) + \mathbf{n}(i,j), \tag{4.15}$$

$$\mathbf{n}(i,j) = [n_1(i,j),\, n_2(i,j)]^T, \tag{4.16}$$

$$\mathbf{H}_X(i) = [H_{X_1}(i),\, H_{X_2}(i)]^T, \tag{4.17}$$

$$\mathbf{H}_I(i) = \begin{cases} [H_{I_1}(i),\, H_{I_2}(i)]^T & \forall i \in S_{\text{interf}}, \\ \text{Not defined} & \forall i \in S_{\text{non-interf}}; \end{cases} \tag{4.18}$$

$$i = 1, 2, \ldots, U_{\text{sub}}.$$

Channel estimation and all further signal processing is done in frequency domain, channels $\mathbf{H}_X(i)$ and $\mathbf{H}_I(i)$ are assumed uncorrelated, while correlation ρ_X between channels of IEEE 802.11g $H_{X_1}(i)$ and $H_{X_2}(i)$ and correlation ρ_I between channels of ZigBee $H_{I_1}(i)$ and $H_{I_2}(i)$ is non-zero. Note that for the interference-free IEEE 802.11g subcarriers, ZigBee channels are not defined. Entries of the noise vector $\mathbf{n}(i,j)$ contains components from both thermal noise, which is Gaussian and interference, which is not necessarily Gaussian. However, for this work, we model both noise sources as Gaussian as we did for single antenna case. Besides, the thermal noise variance is assumed to be constant for a given OFDM frame while the noise induced by interferers vary from subcarrier to subcarrier. Without loss of generality, we omit the subcarrier and OFDM symbol indexes (i,j) from notations of the received vector $\mathbf{Y}$, samples X and I and noise vector $\mathbf{n}$ and use them only when required.

4.5.2 Maximal Ratio Combiner and Optimal Combiner

Maximal Ratio Combiner(MRC) is one of the proven methods to increase the SNR of the signals in a multi-antenna receiver [98]. In OFDM systems, MRC is performed on a per-subcarrier basis as follows: [87]

$$Y_{\text{MRC}} = \widehat{\mathbf{H}}_X^H \mathbf{Y}. \tag{4.19}$$

Where Y_{MRC} is the complex sample after performing MRC, and $\widehat{\mathbf{H}}_X$ denotes the estimated channel. Although, MRC is capable of providing diversity gain the presence of uncorrelated multi-path fading and array gain in case of correlated fading, the performance of MRC severely degrades in the presence of CCI [98].

Optimal Combiner is a superset of MRC which, in the presence of colored noise (interference), additionally computes Interference-plus-Noise (IPN) correlation matrix across all the receive antennas and nullifies the interference [98],[87]. In a two antenna system, the optimally combined signal for subcarriers experiencing interference (S_{interf}) can be written as:

$$y_{\text{OC}} = \widehat{\mathbf{h}}_X^H \phi_{RR}^{-1} \mathbf{y}. \tag{4.20}$$

$$\text{Where} \quad \phi_{RR} = \mathbb{E}\{ [\tilde{y}_1, \tilde{y}_2] [\tilde{y}_1, \tilde{y}_2]^H \} \tag{4.21}$$

is the IPN correlation matrix, and $\tilde{y}_1$ and $\tilde{y}_2$ are received signals on first and second WiFi-Rx antenna respectively when only ZB-Tx transmits and WiFi-Tx is silent. For the interference-free subcarriers, $\phi_{RR} = \sigma^2 \mathbf{I}$ where $\mathbf{I}$ is $M \times M$ identity matrix and σ^2 is the noise variance. Thus, in the absence of interference, OC acts as MRC [87, Eq-6.92]. The drawback of OC is that computation of ϕ_{RR} needs to be performed for all the interfered subcarriers when only ZB-Tx transmits. Besides, ϕ_{RR} needs to be updated with the period of coherence time of $\mathbf{h}_I$ as it varies with channel fading rate. Both of these conditions are difficult to meet in practice. Moreover, since ϕ_{RR} is a matrix of order M, the computational complexity of matrix inversion grows with the number of antennas M.

4.5.3 Technology Independent MIMO

Technology Independent MIMO (TIMO) [34] applies Zero Forcing (ZF) receive beamforming using two antennas to null the interference. Conventionally ZF receive beamforming requires exact channel estimates of the interferer [35], [88], [14]. In contrast, TIMO uses the channel estimate ratio (β) of the interferer, i.e., $\beta = \widehat{h}_{I_1} / \widehat{h}_{I_2}$. Such property of TIMO makes it suitable for unmanaged networks as obtaining the exact channel estimates of the interferer in unmanaged networks is impossible or very costly due to the unknown structure of the interfering signals. The early work of TIMO ignores noise [34, Eq-5,6] during computation of CER β. Hence, we refer to a recent work on TIMO in [105] where authors consider the noise and use an MMSE estimator to compute CER β for the interfered subcarriers as follows:

$$\beta = \frac{\mathbb{E}\{ (Ih_{I_1} + n_1) \left(Ih_{I_2} + n_2 \right)^H \}}{\mathbb{E}\{ |y_2|^2 \}}. \tag{4.22}$$

Considering an OFDM system, TIMO uses the β to null the interference on interfered subcarriers and obtain the Signal Of Interest (SOI) as follows:

$$y_{\text{TIMO}}^{\text{interf}} = \frac{y_1 - \beta y_2}{\widehat{h}_{X_1} - \beta \widehat{h}_{X_2}}. \tag{4.23}$$

To compute SOI on the interference-free subcarriers, we first compute CER β for the interference-free subcarriers by setting $I = 0$ in (4.22) and since, n_1 and n_2 are uncorrelated, it can be shown that $\beta = 0$ for all the interference-free subcarriers. Hence, SOI for all the interference-free subcarriers $y_{\text{TIMO}}^{\text{non-interf}}$ can be written as:

$$y_{\text{TIMO}}^{\text{non-interf}} = \frac{y_1}{\widehat{h}_{X_1}}. \tag{4.24}$$

Expression (4.24) is the well known Zero-Forcing Equalization (ZFE) over a single antenna [87, Sec-7.3.1.1]. We observe that TIMO fails to exploit the diversity gain for all the interference-free subcarriers which potentially could be achieved using the already available two antennas of the TIMO receiver. Additionally, CER β varies with the fading rate of $\mathbf{h}_I$ and hence needs a continuous update after every channel coherence period. Such requirements are difficult to guarantee in practice.

In the next sections, we discuss our work of [55] where we overcome the limitations of OC and TIMO and develop methods to recover IEEE 802.11g on a multi-antenna receiver facing narrowband ZigBee interference.

4.5.4 Maximum Ratio Combiner with Log-Likelihood Ratio Scaling (MLSC)

In our first method, we propose to perform MRC over signals from the receive antennas. This is followed by scaling the obtained LLRs from MRC combined signal using a vector of Localized Noise Variance (LNV) estimates aggregated over the receive antennas. We term our method as MLSC (**M**aximum Ratio Combiner with **L**og-Likelihood Ratio **SC**aling) for the rest of the work. MLSC receiver benefits from diversity gain as well as interference mitigation simultaneously. For a M antenna IEEE 802.11g receiver, MLSC is performed on a per-subcarrier basis as follows:

1. **Step-1:** Combine the signals from M antenna branches according to MRC as in (4.19) and obtain Y_{MRC}.

2. **Step-2:** Average the LNV vectors obtained from (4.6) over all the antennas as follows:

$$\widehat{\boldsymbol{\sigma}}_{\text{Avg}}{}^2 = \frac{1}{M}\sum_{m=1}^{M}\widehat{\boldsymbol{\sigma}}_m^2. \tag{4.25}$$

   where $\widehat{\boldsymbol{\sigma}}_m^2$ is the noise variance vector corresponding to m-th antenna.

3. **Step-3:** Scale the LLR corresponding to the i-th subcarrier using $\widehat{\sigma}_{\text{Avg}}^2(i)$, which is i-th element of the vector $\widehat{\boldsymbol{\sigma}}_{\text{Avg}}^2$, as follows:

$$\begin{aligned}\Lambda(i,l) = &\frac{\min\limits_{z\in Z_0^l}\left(\left|Y_{\text{MRC}}(i)-(|H_{X_1}(i)|^2+|H_{X_2}(i)|^2)z\right|^2\right)}{\widehat{\sigma}_{\text{Avg}}^2(i)} \\ &-\frac{\min\limits_{z\in Z_1^l}\left(\left|Y_{\text{MRC}}(i)-(|H_{X_1}(i)|^2+|H_{X_2}(i)|^2)z\right|^2\right)}{\widehat{\sigma}_{\text{Avg}}^2(i)}\end{aligned} \tag{4.26}$$

For a dual antenna IEEE 802.11g receiver, the schematic of MLSC is illustrated in Fig. 4.25.

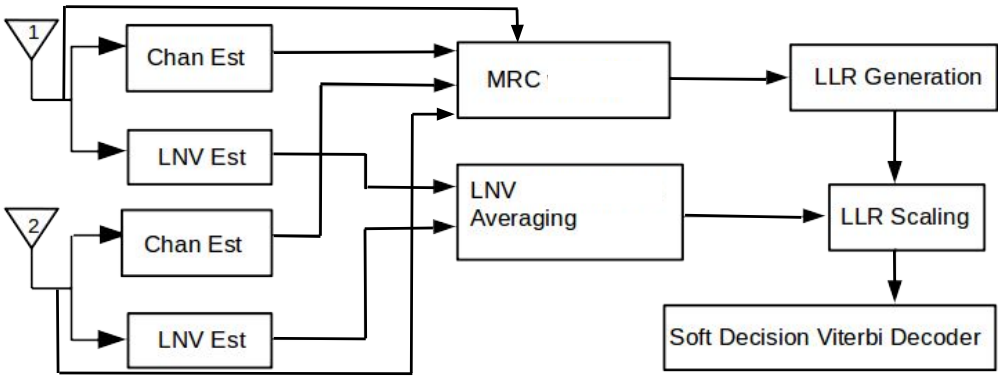


Fig. 4.25. Schematic of Proposed MLSC for 2 Antenna WiFi Receiver

4.5.5 Diversity Combiner TIMO (DC-TIMO)

We have observed in Section 4.5.3 that TIMO does not exploit the potential diversity gain for all the interference-free subcarriers in an OFDM system. We propose to solve this issue by performing MRC on all the interference-free subcarriers. Our method is very simple and enables a TIMO receiver to benefit from interference nulling on the interfered subcarriers as well as from diversity gain on the interference-free subcarriers simultaneously. We term the proposed method as Diversity Combiner TIMO (DC-TIMO). SOI with DC-TIMO for the interfered subcarriers $y^{\text{interf}}_{\text{DC-TIMO}}$ and the interference-free subcarriers $y^{\text{non-interf}}_{\text{DC-TIMO}}$ is obtained as follows:

$$y^{\text{interf}}_{\text{DC-TIMO}} = \frac{y_1 - \beta y_2}{\widehat{h}_{X_1} - \beta \widehat{h}_{X_2}} \tag{4.27}$$

$$y^{\text{non-interf}}_{\text{DC-TIMO}} = \widehat{\mathbf{h}}_X^H \mathbf{y}. \tag{4.28}$$

4.5.6 Simulations and Results

To validate MLSC and DC-TIMO, we perform Monte Carlo simulations using the standard compliant IEEE 802.11g and IEEE 802.15.4 libraries available in release 2017b of MATLAB. We simulate the worst case scenario, i.e., when lack of CSMA/CA creates a 100% chance of collision. The simulation parameters are mentioned in Table 4.1. For all the experiments, we choose Transmit Power level (TxP) required to achieve 10% PER as our performance metric.

4.5.6.1 Comparing MLSC and OC

We simulate a dual antenna IEEE 802.11g receiver (WiFi-Rx) capable of performing OC and MLSC simultaneously. The WiFi-Rx decodes packets received from a single antenna IEEE 802.11g transmitter (WiFi-Tx) under interference from a single antenna ZigBee transmitter (ZB-Tx) as illustrated in Fig. 4.24. Two different ZigBee TXP levels (-85 and -75) dBm are used. The correlation coefficient ρ_X is fixed to 0.4 based on the measurements of [49]. Since, for both the OC and MRC, the performance is agnostic of ρ_I [32], we fixed it to 0.1. In order to obtain ϕ_{RR} for OC as in (4.20), an expectation was taken over approximately $80,000$ ZigBee samples collected from two receive antennas of WiFi-Rx in order to guarantee the best performance of OC. PER for IEEE 802.11g MCS 0 is plotted in Fig. 4.26. We also plot the PER of conventional MRC under the same setup. We observe that for the mentioned ZigBee TxP (-75 dBm and -85 dBm), the performance of MLSC is quite close to the of OC. The result can be explained by following two facts:

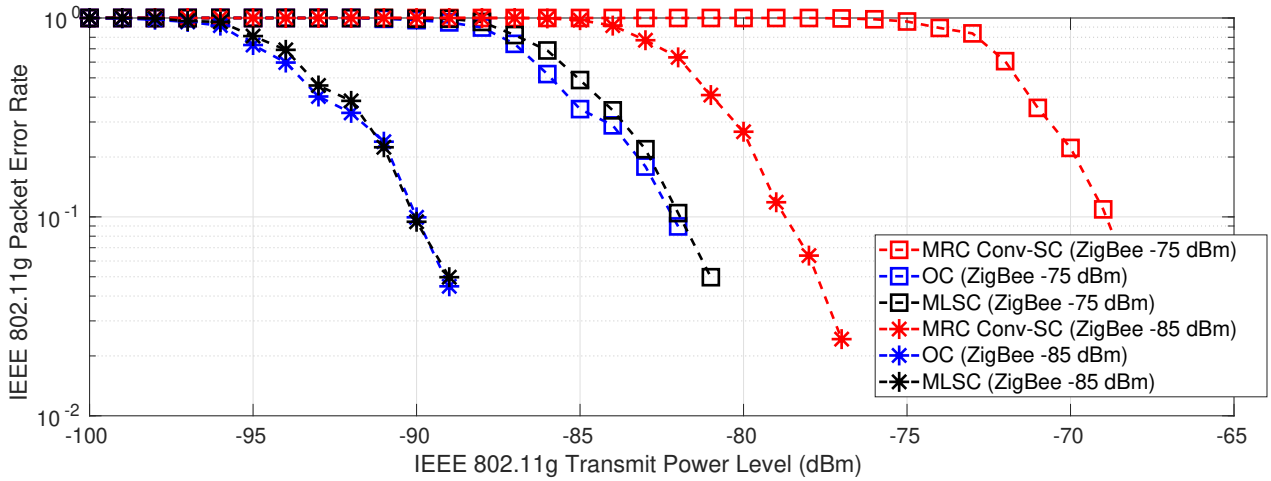


Fig. 4.26. Comparison of MRC (with Conv-SC), OC and MLSC, for IEEE 802.11g MCS 0 and ZigBee TxP -85 dBm

- OC nulls the interference on all the interfered OFDM subcarriers which effectively scales the LLR obtained from all the interfered subcarriers. MLSC performs the same action by directly scaling the LLRs obtained from all the interfered subcarriers in proportion to the LNV estimates.
- For the non-interfered subcarriers, both OC and MLSC boil down to MRC.

The advantage of MLSC over OC is that for a given IEEE 802.11g TxP, MLSC can achieve PER performance very close to the OC but with a lower computational complexity and without the knowledge of the statistics of the interferers.

4.5.6.2 Comparing MLSC and TIMO

We simulate the same scenario as in Section 4.5.6.1 with the difference that now the WiFi-Rx is able to perform TIMO and MLSC simultaneously. IEEE 802.11g MCS 0 and 2 are simulated for a fixed ZigBee TxP of -85 dBm. For TIMO, instead of estimating CER β as in [34, Eq-14], we directly computed it from the channel realization of Zigbee to guarantee the best performance of TIMO. PER is shown in Fig. 4.27 and Fig. 4.28 for IEEE 802.11g MCS 0 and 2 respectively. As a reference, we also plot the PER when the two branches are combined using MRC and the corresponding LLRs are scaled using Conv-SC. We observe that at the best, PER of TIMO is equivalent to MRC; however the performance degrades as the IEEE 802.11g MCS goes high. On the other hand, MLSC provides better PER compared to both MRC and TIMO. The key advantage of MLSC over TIMO is that MLSC does not require the channel estimate ratio of the interferer.

4.5.6.3 Comparing TIMO and DC-TIMO

We simulate the same scenario as in Section 4.5.6.2 except now the WiFi-Rx is able to perform TIMO and DC-TIMO simultaneously. IEEE 802.11g MCS 0 is simulated for a fixed ZigBee TxP of -85 dBm. CER β was computed directly from the channel realization of ZigBee to guarantee the best performance of TIMO. PER is shown in Fig. 4.29. We observe that for a given TxP of IEEE 802.11g, DC-TIMO achieves lower PER than normal TIMO which fails to benefit from the diversity gain. Improvisation from TIMO to DC-TIMO is very simple, yet the gain is notable when a wideband OFDM system gets interference by a narrowband signal.

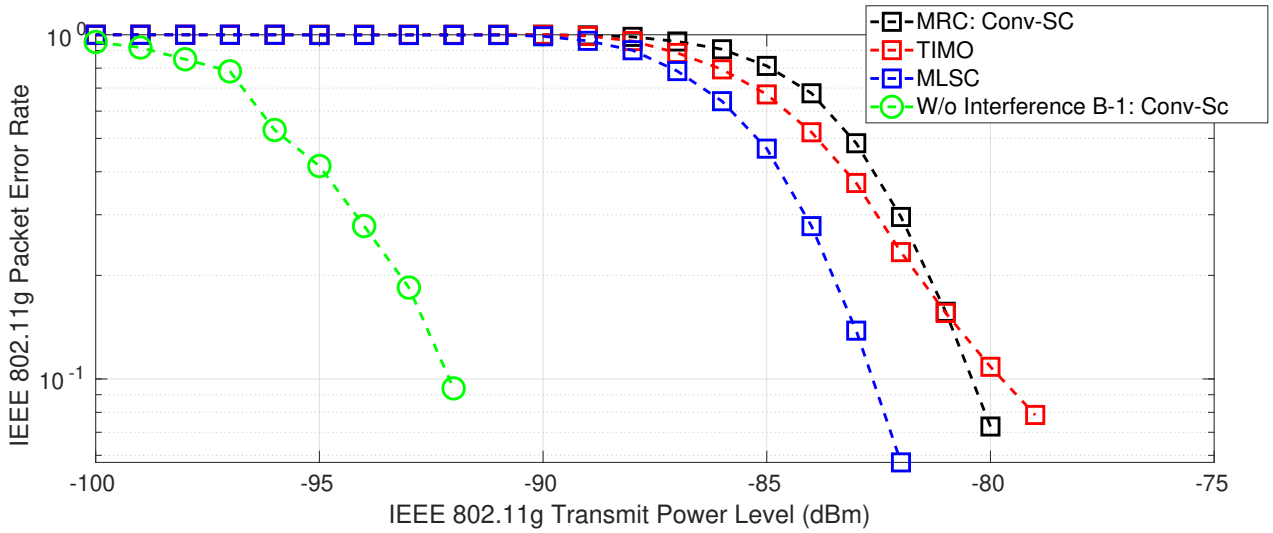


Fig. 4.27. Comparison of MRC(with Conv-SC), MLSC and TIMO for IEEE 802.11g MCS 0. MLSC performs better than both MRC (with Conv-SC) and TIMO. ZigBee TxP −85 dBm

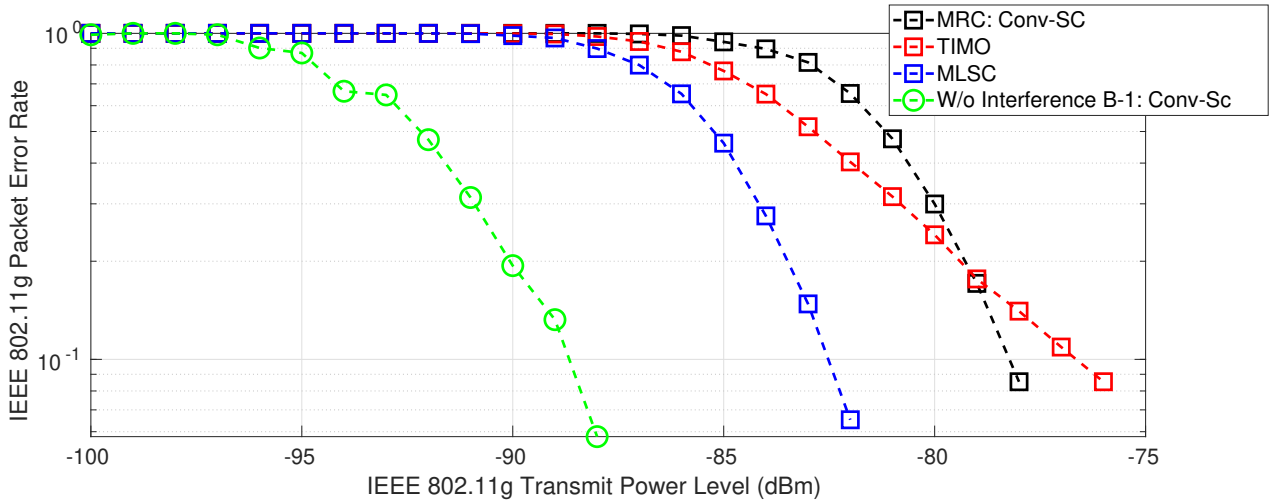


Fig. 4.28. Comparison of MRC(with Conv-SC), MLSC and TIMO for IEEE 802.11g MCS 2. MLSC performs better than both MRC (with Conv-SC) and TIMO. ZigBee TxP −85 dBm

4.5.7 Discussion

- OC, although well known to null the CCI in a multi-antenna system, is practically not feasible to implement due to computational complexity of IPN correlation matrix. In contrast, MLSC achieves the same performance level as OC without knowing the statistics of the interferer. In addition, practically it is possible to implement MLSC using SDR which is detailed in Chapter 7. We use an implementation friendly method of MRC termed as Soft Bit Maximal Ratio Combiner which is discussed in Appendix B.2.

- Likewise MLSC, TIMO is also practically feasible to implement in SDR as discussed by authors in [34] and improves the PER in the event of interference. Obtaining the Channel Estimate Ratio (CER) is practically possible because both IEEE 802.11g and ZigBee apply CSMA/CA providing ample opportunities to measure the CER.

- In addition, DC-TIMO which is obtained by simple modifications to TIMO, shows notable performance gain compared to TIMO. However, in the presence of an interference whose bandwidth

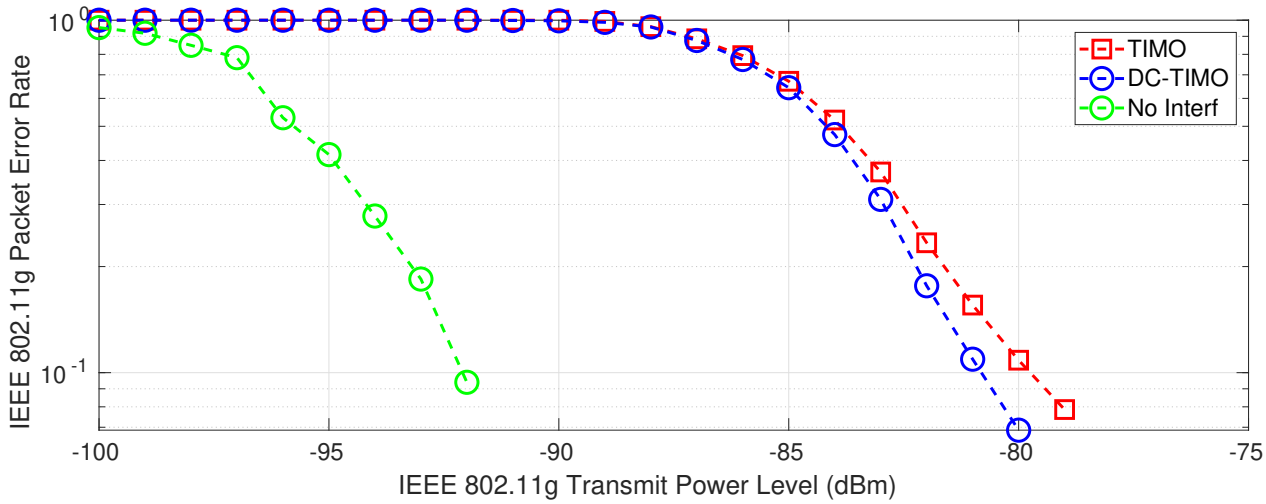


Fig. 4.29. Comparison of TIMO and DC-TIMO for IEEE 802.11g MCS 0. DC-TIMO benefits from the additional diversity gains. ZigBee TxP −85 dBm

is comparable to the wideband OFDM, gain provided by DC-TIMO will be similar to TIMO.

In all the previous sections, our SOI was IEEE 802.11g. In the following sections, we make ZigBee as our SOI and develop methods for its recovery while it faces CCI from IEEE 802.11g.

4.6 Mitigating CCI in Single Antenna ZigBee receiver caused by IEEE 802.11g

Although ZigBee is inherently robust compared to IEEE 802.11g due to usage of spread spectrum technique, the higher transmit power of IEEE 802.11g may result in severe PER degradation as seen in previous works and shown in Fig. 4.9. In this section, we attempt to mitigate interference in a single antenna ZigBee receiver caused by single antenna IEEE 802.11g transmitter. We chose Successive Interference Cancellation (SIC) as our candidate method.

4.6.1 Successive Interference Cancellation of IEEE 802.11g from ZigBee

Referring (4.8) the Signal to Interference plus Noise Ratio (SINR) of ZigBee in the received signal $r[n]$ is:

$$\mathrm{SINR}_{\mathrm{ZB}}[n] = \frac{\mathbb{E}\{|h^z[n] * s^z[n]|^2\}}{\mathbb{E}\{|h^w[n] * s^w[n]|^2\} + \sigma^2}. \tag{4.29}$$

With this $\mathrm{SINR}_{\mathrm{ZB}}$, the detection and decoding of a ZigBee frame depend on the strength of the IEEE 802.11g interference. In order to increase $\mathrm{SINR}_{\mathrm{ZB}}$, we apply SIC over $r[n]$. The post-processing SINR of the weaker ZigBee signal is likely to exceed the required receiver sensitivity [71] of ZigBee receiver, and thus could be decoded. Transmit power of IEEE 802.11g is 5-20 dBm [101] higher compared to ZigBee which makes the application of SIC to recover weaker ZigBee from stronger IEEE 802.11g favorable. The process of SIC starts when a strong IEEE 802.11g signal is detected and decoded at the receiver. During the process of decoding, the channel estimates of IEEE 802.11g, which are obtained from L-LTS, are stored. Once the decoded bits are available, the stored channel estimates are used to regenerate IEEE 802.11g back. We explain the process as follows:

After the frame detection and N point ($N = 64$ for IEEE 802.11g) FFT of received samples, the frequency domain complex sample $R^w[k]$ on k^{th} subcarrier of IEEE 802.11g is:

$$R^w[k] = H^w[k]X^w[k] + H^z[k]I^z[k] + N[k], \tag{4.30}$$

where $X^w[k]$, $I^z[k]$ are frequency domain IEEE 802.11g and ZigBee symbols respectively. The elements of $R^w[k]$ corresponding to the pilot subcarriers are used to compute estimates $\hat{H}^w$ of the actual channel H^w. Assuming that SINR of IEEE 802.11g is strong enough to allow the frame to pass the Cyclic Redundancy Check (CRC), the next step is to regenerate the IEEE 802.11g frame for its sequential cancellation from the time domain received signal $r[n]$. The regenerated frequency domain received baseband IEEE 802.11g signal $Y^w_{\text{Reg}}[k]$ can be written as:

$$Y^w_{\text{Reg}}[k] = X^w[k]\hat{H}^w[k]. \tag{4.31}$$

We use X^w and not the estimates because we regenerate only those IEEE 802.11g frames which have passed CRC. We then convert $Y^w_{\text{Reg}}[k]$ into the time domain $y^w_{\text{Reg}}[n]$ by performing 64 point IFFT which results in:

$$y^w_{\text{Reg}}[n] = \hat{h}^w[n] * s^w[n]. \tag{4.32}$$

Here $\hat{h}^w[n]$ represents the time domain estimate of the IEEE 802.11g channel. After SIC of estimated IEEE 802.11g interference the residue signal is now:

$$\begin{aligned} r^{\text{SIC}}[n] &= r[n] - y^w_{\text{Reg}}[n] \\ &= h^z[n] * s^z[n] + (h^w[n] - \hat{h}^w[n]) * s^w[n] + v[n]. \end{aligned} \tag{4.33}$$

After SIC the effective SINR of weaker ZigBee becomes

$$\text{SINR}^{\text{SIC}}_{\text{ZB}}[n] = \frac{\mathbb{E}\{|h^z[n] * s^z[n]|^2\}}{\mathbb{E}\{|(h^w[n] - \hat{h}^w[n]) * s^w[n]|^2\} + \sigma^2}. \tag{4.34}$$

From (4.34), it can be observed that the more accurate the channel estimate $\hat{h}^w$, the smaller is the noise term $\mathbb{E}\{|(h^w - \hat{h}^w) * s^w|^2\} + \hat{\sigma}^2$ in the denominator and the higher is post processing SINR of ZigBee, i.e., $\text{SINR}^{\text{SIC}}_{\text{ZB}}$. Note that sampling rate of $r^{\text{SIC}}[n]$ is 20 MHz; hence before sending it to ZigBee receiver it has to be downsampled at 2 MHz.

4.6.2 Simulations and Results

To validate performance of SIC in recovering ZigBee, we perform Monte Carlo simulations using the standard compliant IEEE 802.11g and IEEE 802.15.4 libraries available in release 2017b of MATLAB. Interference is caused by single channel IEEE 802.11g whose TxP is fixed to -85 dBm. We performed simulations for IEEE 802.11g MCS 0 and 2 We use 10% PER mark as our performance metric. Simulation parameters were same as mentioned in Table 4.1. Plots are shown in Fig. 4.30 and Fig. 4.31. From the plots, we observe that SIC of IEEE 802.11g in the event of interference provides approx 4 dB of gain compared to the case when SIC is not performed. The gain is consistent for all the IEEE 802.11g MCS. Consistency with respect to MCS is obvious as the performance depends on the post-processing SINR of ZigBee which is independent of the MCS of IEEE 802.11g.

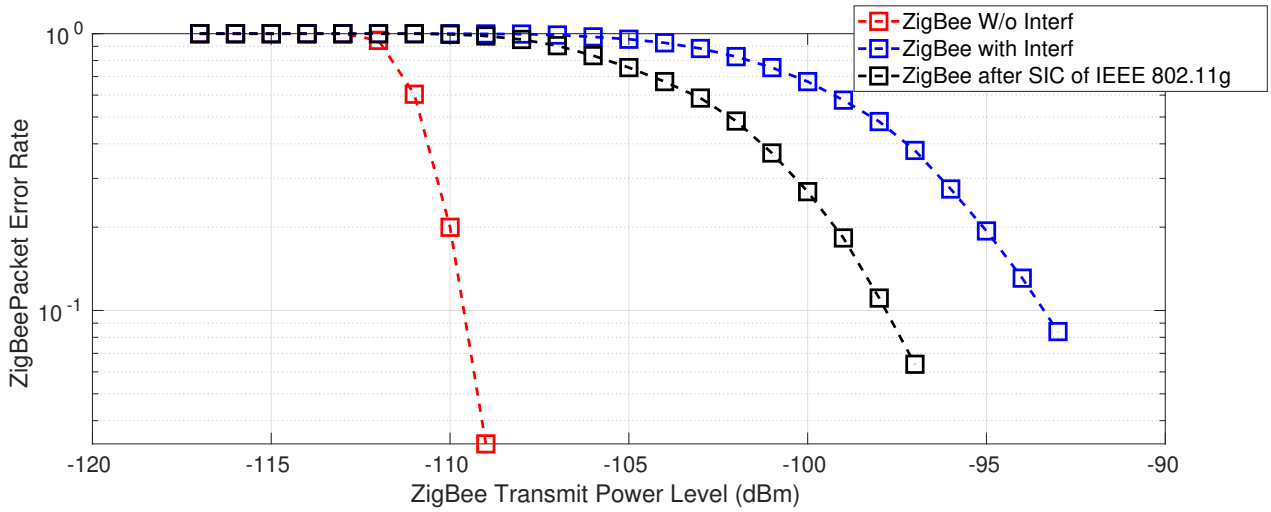


Fig. 4.30. PER of ZigBee after SIC of single channel IEEE 802.11g(MCS 0, TxP −85 dBm).

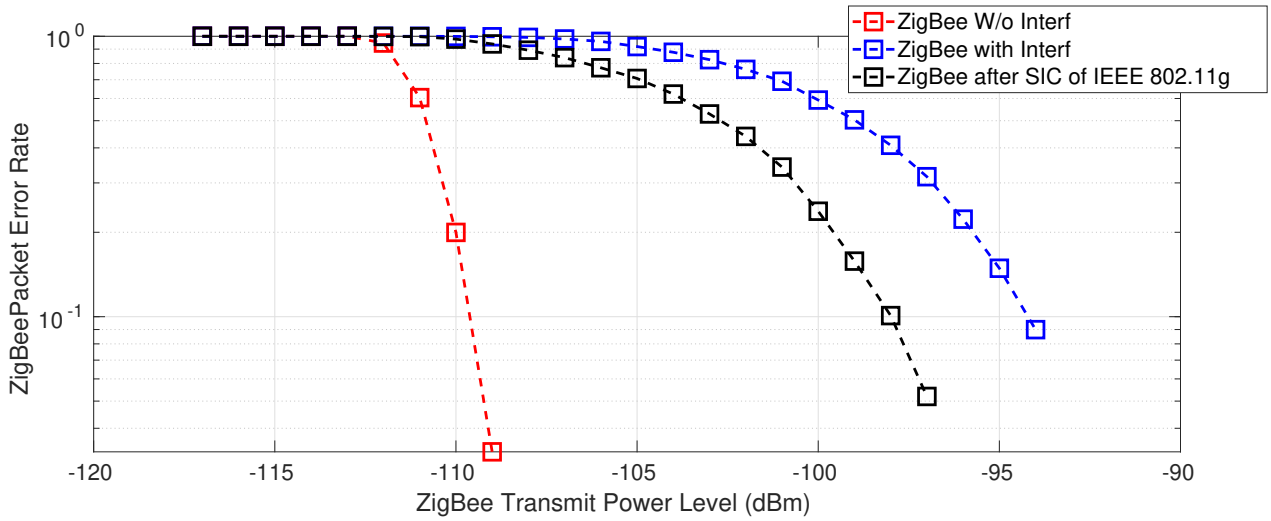


Fig. 4.31. PER of ZigBee after SIC of single channel IEEE 802.11g (MCS 2, TxP −85 dBm).

4.6.3 Discussion

SIC shows positive results during CT-CCI. In the coming sections, we will see the benefits of SIC for other signals with different physical layers also. However, the performance of SIC is dependent on how accurately the stronger signal has been regenerated which in turn depends on how accurate the channel estimates of the stronger signal are. In the event of interference, the accuracy of channel estimates get affected [47] resulting in reduction of the post-processing SINR of the weaker signal. Additionally, as the number of ZigBee channels grows, post-processing SINR will further decrease. In the next section, we present multi-antenna signal processing methods to overcome this limitation and improve the performance of ZigBee SIC receiver through diversity gain.

4.7 Mitigating CCI in Multi-Antenna ZigBee receiver caused by IEEE 802.11g

We have already seen the benefits of multi-antenna signal processing algorithms MLSC, TIMO and DC-TIMO to mitigate CT-CCI. Also we have seen the benefits of SIC for single antenna ZigBee receiver in Section 4.6.1. In this section, we develop SIC methods for multi-antenna ZigBee receivers.

4.7.1 SIC of IEEE 802.11g followed by MRC of ZigBee

SIC of IEEE 802.11g is effective in recovering the buried ZigBee signals as we have seen in Section 4.6.1. However, the performance of SIC depends on the post-processing SINR of ZigBee which in turn depends on channel estimation accuracy of the IEEE 802.11g signal. In the presence of ZigBee interference, channel estimation accuracy of IEEE 802.11g is affected which increases the noise term in the denominator of (4.34), i.e., $\mathbb{E}\{|(h^w[n]-\hat{h}^w[n]) * s^w[n]|^2\} + \sigma^2$. To reduce this noise, we propose to perform MRC over ZigBee after the SIC of IEEE 802.11g. We start with the previous receiver structure and extend it for a dual antenna receiver and perform SIC of IEEE 802.11g over both the antenna branches. Following to that, we perform frame synchronization of ZigBee on both the branches. Once frames are detected, MRC of the ZigBee signals is performed to reduce the noise induced by inaccurate channel estimation of IEEE 802.11g. We term this receiver structure as **SIC-MRC** for the rest of this work. A typical SIC-MRC receiver is shown in Fig. 4.32.

4.7.2 Simulations and Results

For the following experiments, we have the simulation settings, i.e. channel model for IEEE 802.11g and ZigBee, payload lengths as in the previous simulations.

4.7.2.1 SIC-MRC

We simulate a dual antenna ZigBee receiver being interfered by a single antenna IEEE 802.11g transmitter whose TxP level is fixed to -85 dBm. We use 10% PER mark as our performance metric. In addition, we perform MRC over the two antenna branches of ZigBee without SIC. Results are plotted for IEEE 802.11g MCS 0 and MCS 2 in Fig. 4.33 and Fig. 4.34 respectively. From the plots, we first observe that SIC-MRC provides notable gain over plain SIC due to the fact that post-SIC MRC reduces the residual noise induced by inaccurate channel estimation of the stronger signal. In addition, we see that even plain MRC is capable of reducing the PER in the event of interference.

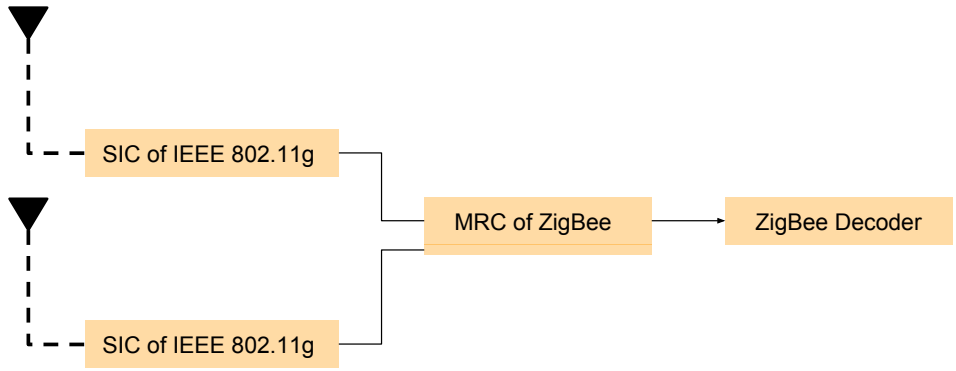


Fig. 4.32. Schematic of SIC-MRC Receiver when IEEE 802.11g is the stronger signal and ZigBee is the weaker signal

.

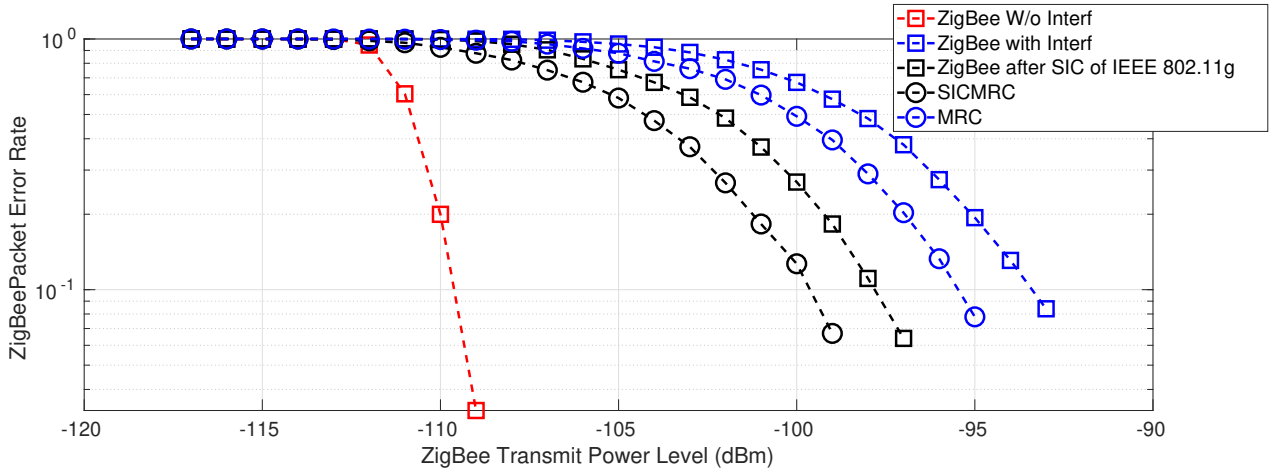


Fig. 4.33. PER comparison of ZigBee when SIC, SIC-MRC and Only MRC is applied, at IEEE 802.11g MCS 0, TxP −85 dBm. SIC-MRC performs better than SIC. Plain MRC is also capable of reducing PER in the event of interference.

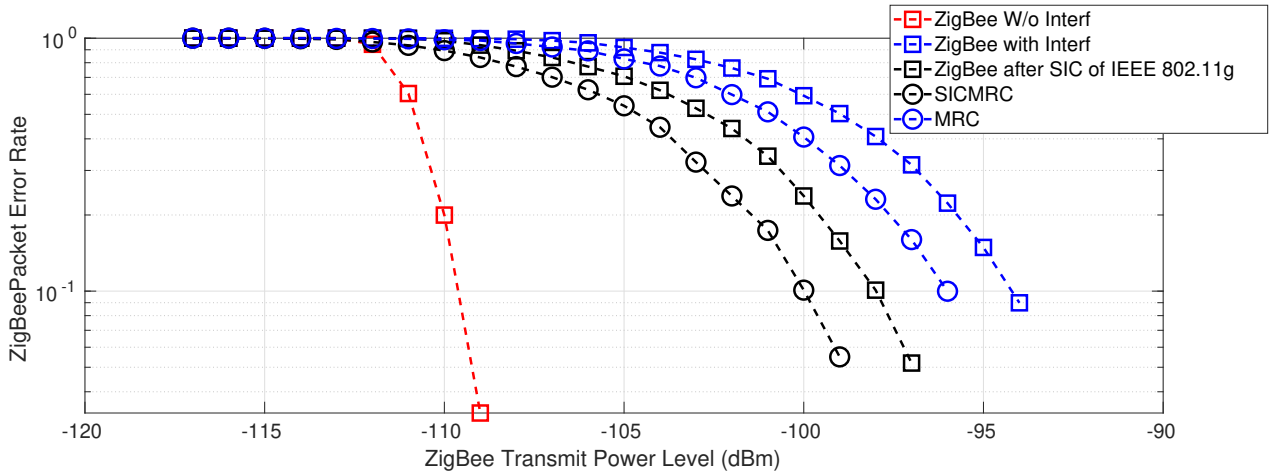


Fig. 4.34. PER comparison of ZigBee when SIC, SIC-MRC and Only MRC is applied, at IEEE 802.11g MCS 2, TxP −85 dBm. SIC-MRC performs better than SIC. Plain MRC is also capable of reducing PER in the event of interference.

Table 4.5: Methods to detect interference

CT-CCI Detection Method	**Applies to**	**Detects the presence or appearance of interferer**	**Limitations**
Noise Level Ratio (NLR) between LNV estimates of interfered and non-interfered wideband OFDM subcarriers	Wideband OFDM signal facing interference from single and multiple narrowband signals	Already present interferer	Preamble of wideband OFDM which is used to estimate LNV is required to interfere with narrowband signal
Error Vector Magnitude between received signal and regenerated signal	Agnostic of the signal type	Already present as well as appearing interferer	Instantaneous detection of interference is not possible without decoding the data first

Finally, we observe that the benefits of SIC-MRC and MRC are agnostic with respect to the MCS of IEEE 802.11g.

4.7.3 Discussions

In our previous discussion on the limitations of SIC in Section 4.6.3, we mentioned the excess noise induced due to channel estimation inaccuracy of the stronger signal in the event of interference. SIC-MRC proves itself effective in reducing such noise and increases the SINR of the weaker signal. This results in reduced PER of the weaker signal. Although SIC-MRC is superior to SIC;however, it is a complex operation and performing SIC on both antenna branches may further increase the complexity. Interestingly we observed that a plain MRC could also provide gain in the presence of interference. Hence depending on the available signal processing resources, a choice can be made among SIC-MRC or plain MRC in a multi-antenna ZigBee receiver. In the next chapter, we continue our experiments with SIC, MRC and SIC-MRC for the case of interference between two wideband OFDM signals.

4.8 Summary of the Methods

A summary of CT-CCI detection methods and CT-CCI mitigation methods is given in Table 4.5 and Table 4.6 respectively.

Table 4.6: Methods to Mitigate CT-CCI between wideband OFDM and narrowband signals

Interference Mitigation Method	**Interference Scenario**	**Number of Rx Antennas**	**Recovers**	**Re-Sync of weaker signal**	**Comments**
Log Likelihood Scaling of wideband OFDM signal with Localized Noise Variance Estimates (LNV-SC)	Single antenna wideband OFDM signal facing interference from single or multiple narrowband signals	1	Wideband OFDM	No	May assist in SIC of wideband OFDM signal to recover narrowband signal by increasing the number of clean OFDM frames
Maximal Ratio Combining followed by Log Likelihood Ratio Scaling of the wideband OFDM signal using Localized Noise Variance Estimates (MLSC)	Multi-Antenna wideband OFDM signal facing interference from single or multiple narrowband signals	2	Wideband OFDM	No	Same as above
Technology-Independent MIMO (TIMO)	Same as above	2	Wideband OFDM and narrowband	No	May assist in SIC of the stronger signal
Diversity Combiner Technology-Independent MIMO (DC-TIMO)	Same as above	2	Wideband OFDM and narrowband	No	May assist in SIC of the stronger signal
Successive Interference Cancellation of stronger signal (SIC)	Single antenna narrowband signal facing interference from single antenna wideband OFDM signal	1	Wideband OFDM and narrowband	Yes	Wideband OFDM signal needs to be stronger than the narrowband signal.
Successive Interference Cancellation of the stronger signal followed by Maximal Ratio Combining of the weaker signal (SIC-MRC)	Multi-Antenna receiver of the narrowband signal facing interference from the single antenna wideband OFDM signal	2	Wideband OFDM and narrowband	Yes	Wideband OFDM signal needs to be stronger than the narrowband signal.

4.9 Publications

- Kumar, Sumit; Kaltenberger, Florian; Ramirez, Alejandro; Kloiber, Bernhard: **A robust decoding method for OFDM systems under multiple co-channel narrowband interferers** EuCNC 2018, 27th European Conference on Networks and Communications, June 18-21, 2018, Ljubljana, Slovenia

- Kumar, Sumit; Kaltenberger, Florian; Ramirez, Alejandro; Kloiber, Bernhard: **Robust OFDM diversity receiver under co-channel narrowband interference** WIMOB 2018, 14th International Conference on Wireless and Mobile Computing, Networking and Communications, 15-17 October 2018, Limassol, Cyprus

- (Submitted) Kumar, Sumit; Kaltenberger, Florian; Ramirez, Alejandro; Kloiber, Bernhard: **An SDR Implementation of WiFi Receiver for Mitigating Multiple Co-Channel ZigBee Interferers** Submitted to EURASIP Journal on Wireless Communications and Networking, Special Issue on "Systems and Networks for 5G Implementation."

Chapter 5

CT-CCI Mitigation Between Two OFDM Signals

This chapter focus on the CT-CCI between two wideband OFDM signals and develops corresponding interference mitigation techniques. We have chosen 20 MHz IEEE 802.11ac and 20 MHz LTE-LAA (Long Term Evolution Licensed Assisted Access). Both are wideband OFDM signals and operate in 5 GHz ISM band and are prone to CCI. We develop CT-CCI methods for single and multi-antenna receivers to recover LTE-LAA and IEEE 802.11ac frames in the event of collision.

5.1 Physical Layer of IEEE 802.11ac and LTE-LAA

Currently, cellular communication is dominated by LTE. LTE is spectrally efficient, and a single antenna LTE link can provide throughput up to 75 Mbps [1] in the downlink [42]. To fulfill the exponential growth of mobile traffic demands, 3GPP has standardized the use of LTE in the 5 GHz unlicensed band in the Release 13 dedicated to LTE Licensed-Assisted Access (LTE-LAA). The 5 GHz ISM band contains massive amount of bandwidth (approx 600 MHz). However, the 5 GHz band is already crowded by the incumbent IEEE 802.11n, IEEE 802.11ac, and the upcoming IEEE 802.11ax (by end of 2019). To address this issue, 3GPP has decided to make Listen Before Talk (LBT) as a mandatory feature in LTE-LAA. Apart from LBT, Qualcomm has proposed other methods for allowing co-existence such as Carrier Sense Adaptive Transmission (CSAT) and Absolute Blank Subframes (ABS) [29]. Previous works and field trials have also shown that in the event of interference between IEEE 802.11ac and LTE-LAA, IEEE 802.11ac becomes the primary victim [40], [58].

5.1.1 IEEE 802.11ac

IEEE 802.11ac, also known as **WiFi-5** was induced in 2013 as a Very High-Throughput (VHT) WLAN in the 5 GHz ISM band [86]. Frequency allocation of IEEE 802.11ac is same as IEEE 802.11n and is shown in . Fig. 5.1. In Fig. 5.1, DFS stands for Dynamic Frequency Selection and the

[1] SISO 20 MHz mode

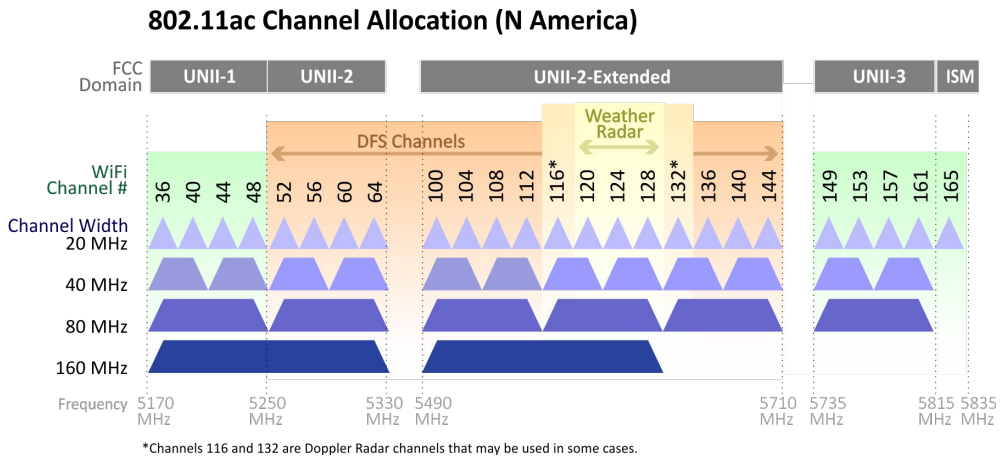


Fig. 5.1. Frequency Allocation of IEEE 802.11ac in 5 GHz band (FCC, North America)

VHT Frame Format

L-STF	L-LTF	L-SIG	VHT-SIG-A	VHT-STF	VHT-LTF	VHT-SIG-B	SERVICE bits	Payload	Pad bits	Tail bits

Fig. 5.2. IEEE 802.11 VHT Frame Format

devices operating on the corresponding bands have to apply Transmit Power Control in order to avoid interference with weather radars and military equipments, if found nearby(reference). IEEE 802.11ac provides backward compatibility with all the previous OFDM based IEEE 802.11 family. Hence the frame format of IEEE 802.11ac appends over the frame format of IEEE 802.11a/g/n. VHT frame format of IEEE 802.11ac is shown in Fig. 5.2. Minimum operational bandwidth of IEEE 802.11ac is 20 MHz; nonetheless, it can be increased up to 160 MHz through channel bonding [95]. For 20 MHz IEEE 802.11ac, L-STF, L-LTF, and L-SIG are the same OFDM symbols as in IEEE 802.11 a/g/n. VHT-SIG-A field contains the information required to interpret VHT format packets such as actual rate value, channel coding, guard interval, MIMO scheme, and other configuration details for the VHT format packet. VHT-STF is a single OFDM symbol (4us in length) that is used to improve automatic gain control estimation in a MIMO transmission. VHT-LTF is used for MIMO channel estimation and pilot subcarrier tracking. The VHT-LTF includes one VHT long training symbol for each spatial stream indicated by the selected MCS. The VHT-SIG-B field is used for the multiuser scenario to set up the data rate and to fine-tune MIMO reception and contains the actual rate and payload length per user. VHT-Data field contains the payload while Service, tail and Pad bits play the same role as their HT (High Throughput) and non-HT (Non-High Throughput) counterparts in IEEE 802.11n and IEEE 802.11a/g respectively.

IEEE 802.11ac uses 64 point FFT for the 20 MHz band giving 64 OFDM subcarriers out of which 56 subcarriers are used for Data(52) and Pilots (4)[2]. Each OFDM symbol of IEEE 802.11ac

[2]Non-HT WiFi, i.e., IEEE 802.11a/g and HT WiFi, i.e., IEEE 802.11n uses 52 subcarriers for Data (48) and Pilots (4)

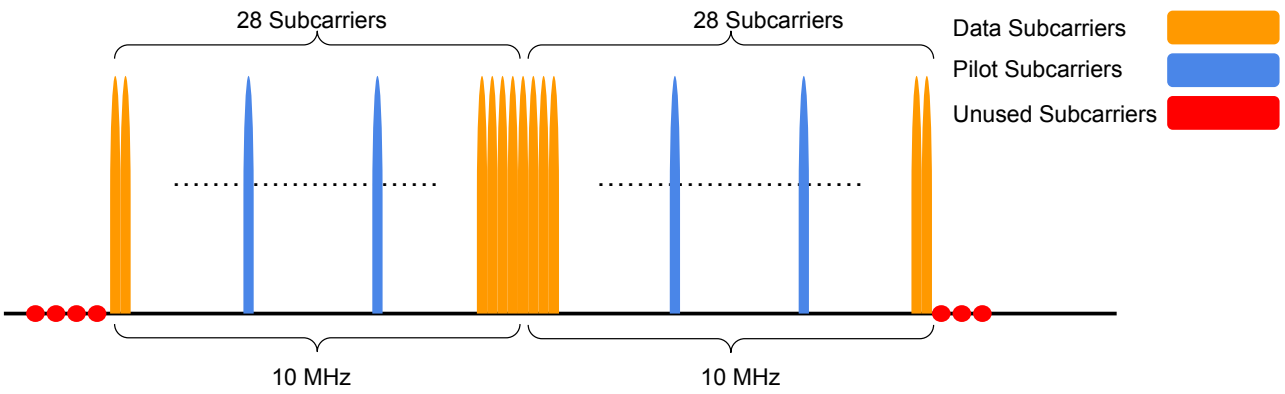


Fig. 5.3. IEEE 802.11ac subcarrier allocation

is 4us long. Fig. 5.3 shows the subcarrier allocation of IEEE 802.11ac in the 20 MHz band. To the left, 4 and to the right and 3 subcarriers are unused to help isolate against adjacent channels. Similarly, the DC subcarrier is left used to avoid DC leakage due to the usage of low-cost Direct conversion receivers. 20 MHz bandwidth of IEEE 802.11ac supports BPSK, QPSK, 16QAM, 64QAM and 256QAM modulation schemes.

5.1.2 LTE-LAA

LTE-LAA is the 3GPP standardized version of LTE-U (LTE in Unlicensed band). LTE-U did not have the provision to listen before talk (LBT), and experimental evaluations showed severe performance degradation of WiFi in the presence of LTE-U [20]. In LTE-LAA, 3GPP has made Listen Before Talk (LBT) as a mandatory feature. LBT is similar to CSMA/CA where the transmitter has to sense the channel before it transmits to check whether the channel is free or occupied. The LTE-LAA air interface is based on OFDM for downlink and a Single-Carrier Frequency Division Multiple Access (SC-FDMA) for the uplink. For 20 MHz of bandwidth, the sampling rate of LTE-LAA is 30.72 MHz, and it applies 2048 point FFT to generate the OFDM signal. The operating bandwidth is approximately 20 MHz because only 1200 subcarriers out of 2048 subcarriers are used. After coding and modulation, a transformed version of the complex-valued modulated signal termed as resource element is mapped on to a time-frequency coordinate system called resource grid. It is a time-frequency grid which is shown in Fig. 5.4. The resource grid has time on the x-axis and frequency on the y-axis. In the time domain, LTE-LAA is structured as frame and subframes which is shown in Fig. 5.5. Each frame is 10 ms in duration and consists of 10 subframes 1 ms each. Further, each sub-frame is composed of two slots, 0.5 ms each. Finally, each slot consists of OFDM symbols, either seven or six depending on whether a normal or an extended cyclic prefix has been used. In the frequency domain, LTE-LAA is structured as resource blocks. Each resource block is made of 12 OFDM subcarriers, hence, 180 KHz wide. 20 MHz LTE-LAA consists of 100 such resource blocks, hence occupies 18MHz of used bandwidth out of 20 MHz usable bandwidth. Some of the subcarriers are left unused to both

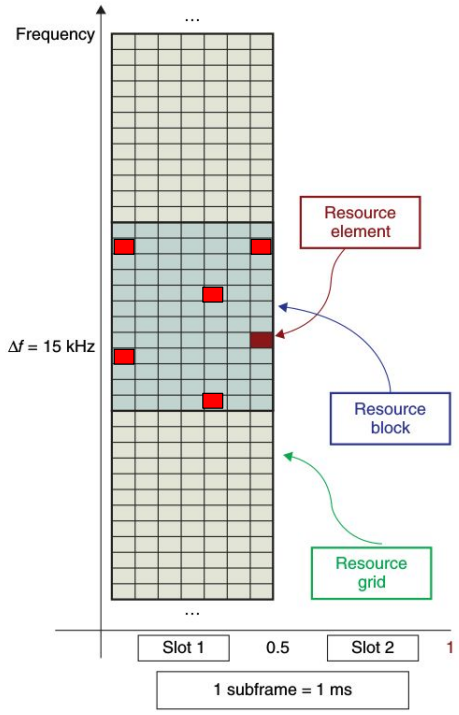


Fig. 5.4. LTE-LAA Downlink Resource Grid

sides of the spectrum to relax the front-end filtering requirements. Channel estimation in LTE-LAA is performed using Cell-Specific Reference Signals which are embedded in both time and frequency domain inside a resource grid as shown by red dots in Fig. 5.4. For frame synchronization, timing offset correction and frequency offset correction, LTE-LAA uses Primary Synchronization Sequence (PSS) and Secondary Synchronization Sequence (SSS) [85].

5.1.3 Interference Scenarios

Although LTE-LAA uses LBT and IEEE 802.11ac uses CSMA/CA to access the channel, the situation of the hidden terminal and blind terminal [104] persists in the case of LTE-LAA and IEEE 802.11ac

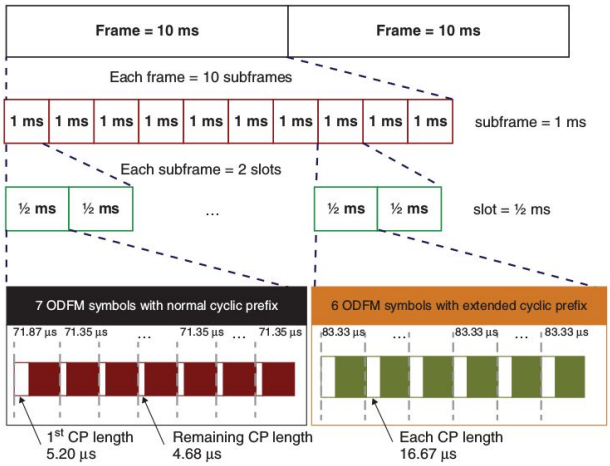


Fig. 5.5. Time Domain LTE-LAA

too. This is also indicated by previous simulations and field trials [103][100]. As there is no provision of RTS-CTS (Request to send and Clear to send), packet exchange between IEEE 802.11ac and LTE-LAA, the performance degradation could be severe.

There are two reasons why a frame is lost during a collision. Frame synchronization failure and Cyclic Redundancy Check (CRC) failure. Frame synchronization is performed using preambles which are very robust in nature as they use the lowest available MCS. IEEE 802.11ac uses BPSK and LTE-LAA uses QPSK to modulate the preambles. At low power, if the collision happens, frame synchronization fails and the frame is never detected. After a certain power level, frame synchronization never fails, i.e., frame is always detected; however, now the frame is prone to CRC failures subjected to the power on interference which also depends on the MCS used by the payload.

Knowing the mutual performance degradation of IEEE 802.11ac and LTE-LAA during simultaneous operation, in the next sections, we proceed towards developing signal processing methods to mitigate the effects of interference and recover both LTE-LAA and IEEE 802.11ac. Our methods reduce both frame synchronization and CRC failures in the event of interference.

5.2 Mitigating CCI in Single Antenna IEEE 802.11ac Receiver Caused by LTE-LAA

In this section, we piggyback on the methods developed in Chapter 4 and use them for the case of IEEE 802.11ac and LTE-LAA with IEEE 802.11ac as our Signal of Interest (SOI). Further we improvise the SIC to increase its effectiveness for indoor deployments where the channel posses slow fading characteristics.

5.2.1 SIC of LTE-LAA CCI from IEEE 802.11ac

In this section, without loosing the generality we assume LTE-LAA as the stronger signal and IEEE 802.11ac as the weaker signal. With the aforesaid assumption, we attempt to recover IEEE 802.11ac by performing SIC of LTE-LAA frm the composite signal. Since, the theory of SIC is already established in Chapter 4 and through simulations its effectiveness in mitigating CT-CCI between wideband OFDM and narrowband signals is proved, we skip the theoretical details of SIC and proceed towards implementation details for the particular case of IEEE 802.11ac and LTE-LAA.

Both IEEE 802.11ac and LTE-LAA standards have the provision of training signals for channel estimation: Cell-Specific Reference Signals for LTE-LAA and VHT-LTF for IEEE 802.11ac. This makes the prototyping a SIC-based receiver for both LTE-LAA and IEEE 802.11ac straightforward. We assume that the LTE-LAA is strong enough such that after colliding with IEEE 802.11ac it is still detected (frame synchronization) and frame boundaries are correctly detected (timing offset detection). After 2048 point FFT, the samples are sent for channel estimation and decoding. Once the

frame passes CRC test, it is regenerated using the stored channel estimates. Next SIC is performed and residue signal is resampled at 20 MHz and fed to IEEE 802.11ac receiver where it goes through usual receiver processing starting with the frame synchronization routines. In Section 5.2.3 we perform simulations to verify the performance of SIC.

In the next section, we improve SIC for low mobility conditions characterized by low Dopper spread in the channels: a typical situation found in indoor environments.

5.2.2 SIC of LTE-LAA CCI from IEEE 802.11ac under Slow Fading Channel (Indoor Environment)

From the discussion in Section 4.6.1, the post processing SINR of the weaker signal depends on the accuracy of the channel of the stronger signal. When LTE-LAA is stronger than IEEE 802.11ac, the post processing SINR of IEEE 802.11ac $\text{SINR}_{\text{W}}^{\text{SIC}}[n]$ can be written as:

$$\text{SINR}_{\text{W}}^{\text{SIC}}[n] = \frac{\mathbb{E}\{|h^W[n] * s^W[n]|^2\}}{\mathbb{E}\{|(h^L[n] - \hat{h}^L[n]) * s^L[n]|^2\} + \sigma^2}. \tag{5.1}$$

where h^W, h^L are the time domain channels; s^W, s^L are the signals corresponding to IEEE 802.11ac and LTE-LAA respectively. $\hat{h}^L[n]$ is the estimated channel of LTE-LAA under interference and σ^2 is the noise variance. Obtaining an accurate estimate of h^L is difficult as LTE-LAA Cell-Specific Reference Signals get corrupted by IEEE 802.11ac interference. Compared to the case of IEEE 802.11g and ZigBee, the CCI between IEEE 802.11ac and LTE-LAA more severely affects the channel estimation as there is an almost full overlap of both the signals. Here we would like to emphasize that up to a certain degree of the imperfect channel estimation; the LTE-LAA receiver is capable of correct detection the data bits using Turbo decoders (likely at the price of an increased number of turbo iterations). Nevertheless, the accuracy of channel estimates is significant for regeneration of LTE-LAA interference to perform SIC.

5.2.2.1 Proposed Method

The most likely deployment of LTE-LAA will be through Small Cells [48]. In a small cell setting, access points of both LTE-LAA and IEEE 802.11ac will be placed inside indoor environment as illustrated in Fig. 5.6[3]. We propose a method to perform SIC by using stored clean channel estimates of stronger signals obtained during an interference-free period. Our approach leverages the high coherence time of the indoor channel. Stating simply: if the channel coherence time is significantly larger than inter-frame-interval (IFI)[4], the channel estimates obtained in the past can be reused in the immediate future, which is the basis of our proposal.

Let t_1 be the time when there is no interference between IEEE 802.11ac and LTE-LAA frames and

[3]In the figure WiFi means IEEE 802.11ac

[4]By IFI we mean the time of arrival of the subsequent frame

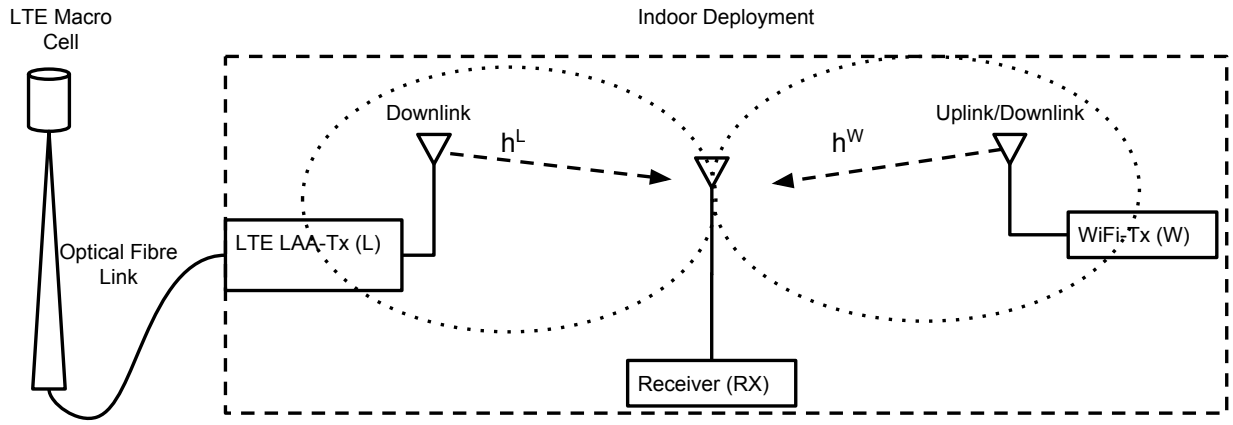


Fig. 5.6. An indoor deployment scenario of single antenna WiFi Tx (W), single antenna LTE-LAA Tx (L) and single antenna WiFi Plus LTE-LAA dual technology receiver (RX)

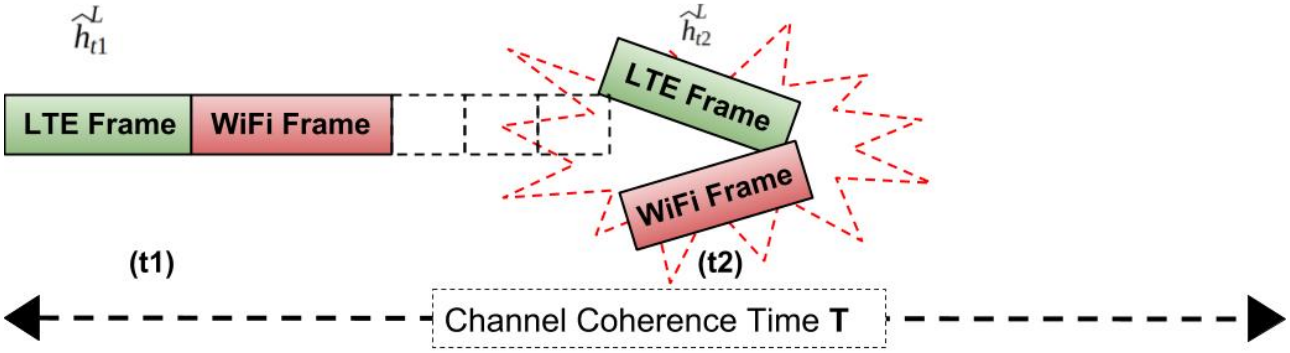


Fig. 5.7. Proposed Scheme to Capture LTE-LAA Channel in the past and apply them in future.

t_2 be the time of interference ($t_2 > t_1$) as shown in Fig. 5.7. Also the LTE-LAA channel estimates at time t_1 and t_2 be $\hat{h}^L_{t_1}$, $\hat{h}^L_{t_2}$ respectively. We propose to regenerate the LTE-LAA interference occured at time t_2 using the interference-free LTE-LAA channel estimates $\hat{h}^L_{t_1}$ obtained at time t_1 in the following two phases:

5.2.2.2 Phase-1: Obtain clean LTE-LAA channel estimates at t_1 when IEEE 802.11ac frame is not being transmitted

Since IEEE 802.11ac uses CSMA/CA and LTE-LAA uses LBT, simultaneous transmission from both of them is already minimized (except the hidden node case). Thus, there will be ample opportunities for the receiver RX (in Fig. 5.6) for listening and decoding the ongoing LTE-LAA transmissions in order to estimate the channel between LTE-LAA transmitter and the receiver. However, an obvious question is how to confirm that the received LTE-LAA frame is interference free?

As discussed before, up to a certain degree of the imperfect channel estimation an LTE-LAA frame can still pass CRC, thanks to the Turbo decoders. CRC failures cannot serve as a reliable indicator of the presence or absence of the interferer because in the low SNR and no interference scenario, the decoding might fail even if the receiver is provided with perfect channel estimates! Neither we can use NLR based interference detection in Section 4.2.5.2 which is used to detect ZigBee's interference

to IEEE 802.11g. The reason being approximately full overlap between both the signals in frequency domain.

5.2.2.3 Interference Detection by EVM Measurements

To register interference, we evaluated RMS of Error Vector Magnitude (R-EVM) between received LTE-LAA samples and regenerated LTE-LAA samples after decoding of the LTE-LAA frames. For a fixed LTE-LAA transmit power (TxP) of -80 dBm and modulation scheme QPSK, we performed simulations to monitor the R-EVM of LTE-LAA in the presence and absence of IEEE 802.11ac frames. We observed that a IEEE 802.11ac signal (MCS-0) with TxP almost near to IEEE 802.11ac receiver sensitivity, i.e., -90 dBm increases the R-EVM of LTE-LAA received signal almost 4 times compared to the R-EVM in the absence of IEEE 802.11ac. Hence, the receiver can be trained to monitor sudden jumps in R-EVM of LTE-LAA signal to reliably find the presence of IEEE 802.11ac interference on those LTE-LAA packets which have passed CRC.

5.2.2.4 Phase-2: Regenerate LTE-LAA interference at t_2 using $\hat{h}^L_{t_1}$ instead of $\hat{h}^L_{t_2}$ if $(t_2 - t_1) << $ T, where T is the LTE-LAA channel coherence time

For LTE-LAA, Extended Pedestrian Model-A (EPA) channel model [69] can be considered as very close approximation of the indoor channel model in terms of Doppler shift. The maximum Doppler shift specified in EPA channel model is 5 Hz which corresponds to a coherence time of approximately 80 ms. This is eight times the duration of a typical LTE-LAA frame duration, i.e., 10 ms (Coherence time = 0.423/Doppler frequency). Assuming the next LTE-LAA frame arrives at time t_2 and $(t_2 - t_1) <<$ T, where T being the channel coherence time, we propose that $\hat{h}^l_{t_1}$ can be reliably used instead of $\hat{h}^l_{t_2}$ to regenerate the LTE-LAA interference which had collided with IEEE 802.11ac frame at t_2. Here the term (t_2–t_1) represents the inter-frame interval (IFI). An illustration of our proposed scheme is shown in Fig. 5.7. Given the knowledge of t_2^{max} over which the operation discussed in **Phase-2** is valid, we explain the proposed receiver operation as follows:

1. The receiver detects an LTE-LAA frame at t_1. It estimates the channel $\hat{h}^l_{t_1}$ and decodes the frame.

2. If the decoded frame passes the CRC and the R-EVM does not exceeds the threshold, the frame is considered interference-free and $\hat{h}^L_{t_1}$ is stored with time stamp t_1.

3. A new LTE-LAA frame is detected at t_2. Its channel is estimated which is $\hat{h}^L_{t_2}$ and the frame is decoded using $\hat{h}^L_{t_2}$.

4. If the frame fails CRC, it is altogether discarded. However, if frame passes CRC and the R-EVM also exceeds the threshold, the presence of a IEEE 802.11ac frame is identified. If the frame passes CRC and R-EVM has not crossed the threshold, clean channel estimates are updated.

5. If t_2 does not exceed t_2^{max}, $\hat{h}_{t_1}^L$ is used to regenerate the LTE-LAA signal instead of $\hat{h}_{t_2}^L$, otherwise $\hat{h}_{t_2}^L$ is used to regenerate the LTE-LAA signal.

6. Finally, the regenerated LTE-LAA interference is canceled from the composite signal and the residue signal is downsampled to 20 MHz and sent for IEEE 802.11ac frame synchronization and decoding.

5.2.3 Simulations and Results

To validate our method, i.e., SIC and SIC for slow fading channels, we perform simulations using the standard compliant IEEE 802.11ac and LTE libraries available in MATLAB Release 2018a. In our experiments, we use 20 MHz LTE bandwidth for the downlink and 20 MHz of 802.11ac bandwidth. For proof of concept, we chose a fixed LTE-LAA TxP of -80 dBm and varied the IEEE 802.11ac TxP. For each IEEE 802.11ac TxP, 100 frames were transmitted. We consider the worst-case scenario as if there is no CSMA/CA or LBT making 100% chance of collision. The simulation parameters are summarized in Table 5.1. As performance metrics we used total number of Synchronization errors and Frame CRC errors.

Table 5.1: Simulation Parameters for LTE-LAA and IEEE 802.11ac Experiments

	802.11ac	**LTE-LAA**
Center Frequency	5 GHz	5 GHz
Bandwidth	20 MHz	20 MHz
Channel	TGac Model-B	EPA
Sampling Rate	20 MHz	30.72 MHz
Payload	500 Bytes	500 Bytes
Modulation and Coding	MCS $0, 2, 4$	QPSK
Noise Power	-100 dBm	-100 dBm

5.2.3.1 Experiment-1: Comparison between SIC with Instantaneous Channel Estimates and No SIC

This experiment is performed to access the gain achieved by performing SIC in the case of CCI between LTE-LAA and IEEE 802.11ac.We compare the performance between SIC with instantaneous channel estimates and no SIC at all. We fixed the TxP of LTE-LAA at -80 dBm, modulation Scheme as QPSK and SIC is performed using instantaneous channel estimates. For every TxP of IEEE 802.11ac, we transmit 100 packets and log the number of received packets[5] which pass CRC. Additionally, we log all the frames which have been detected, i.e., synchronization is successful. First of all, we show the synchronization error plot: with and without SIC. Note that regardless of the MCS used in IEEE 802.11ac, the preamble which is used for packet synchronization is always modulated using BPSK.

[5]We use the term **frame** and **packet** synonymously in this thesis.

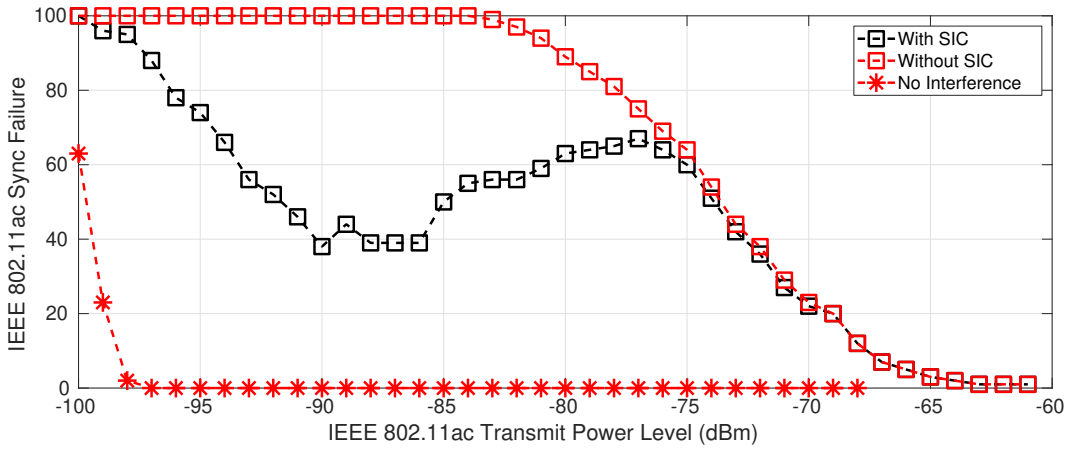


Fig. 5.8. Synchronization error of IEEE 802.11ac MCS 0: With and Without SIC, LTE-LAA −80 dBm. Plot indicates that with SIC, the lost packets of IEEE 802.11ac caused by collision can be recovered.

Hence the synchronization error plot for MCS $0, 2$ and 4 are same. We plot the results for MCS 0 in Fig. 5.8 from which we observe that:

- IEEE 802.11ac synchronization failure significantly increases in the presence of LTE-LAA.
- Applying SIC notably reduces the synchronization failure. Considering a 40% sync failure rate, applying SIC provides $15 - 12$ dB of transmit power gain compared to not applying SIC.
- Synchronization failure increases as the transmit power of IEEE 802.11ac reaches near the transmit power (TxP) of LTE-LAA which is −80 dBm. This happens because as the TxP of IEEE 802.11ac increases, LTE-LAA frames start getting corrupted (CRC test fails) and such frames cannot be regenerated for SIC.

Next we show the frame error plots for IEEE 802.11ac MCS $0, 2$ and 4 in Fig. 5.9, Fig. 5.10 and Fig. 5.11 respectively. From the plots, we observe the following:

- Presence of LTE-LAA significantly degrades the performance of IEEE 802.11ac.
- Performing SIC of LTE-LAA helps in recovering IEEE 802.11ac packets which are lost due to interference. However, the performance of SIC fades with an increase in the constellation size, i.e., the MCS of the weaker signal (IEEE 802.11ac in this case). Because as the MCS increase, the SINR requirement also increases which SIC fails to provide.
- We also observe that as the IEEE 802.11ac TxP reaches near to the TxP of LTE-LAA, i.e., −80 dB, the performance starts degrading. We have observed the same behavior previously in the synchronization plots, and the same reasoning applies for the frame error case also.

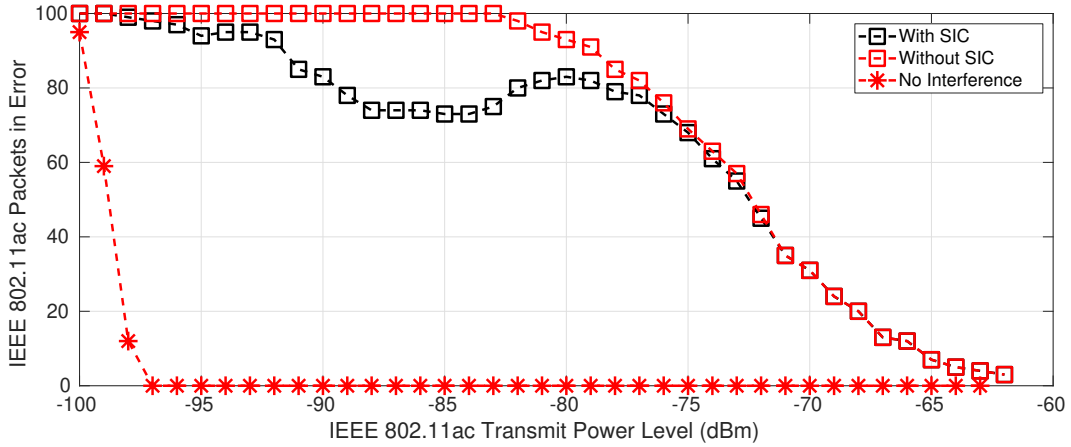


Fig. 5.9. Frame Error for IEEE 802.11ac MCS 0: With and Without Using SIC, LTE-LAA TxP −80 dBm

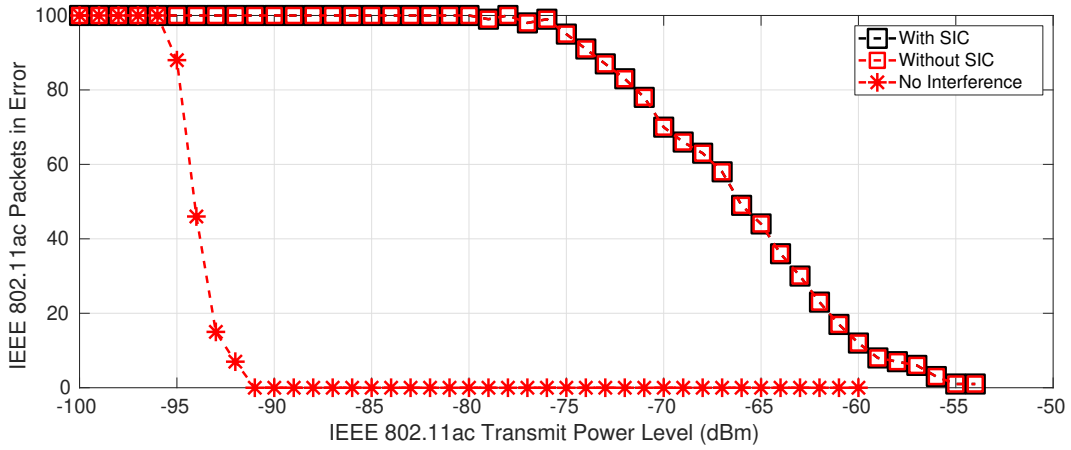


Fig. 5.10. Frame Error for IEEE 802.11ac MCS 2: With and Without Using SIC, LTE-LAA TxP −80 dBm

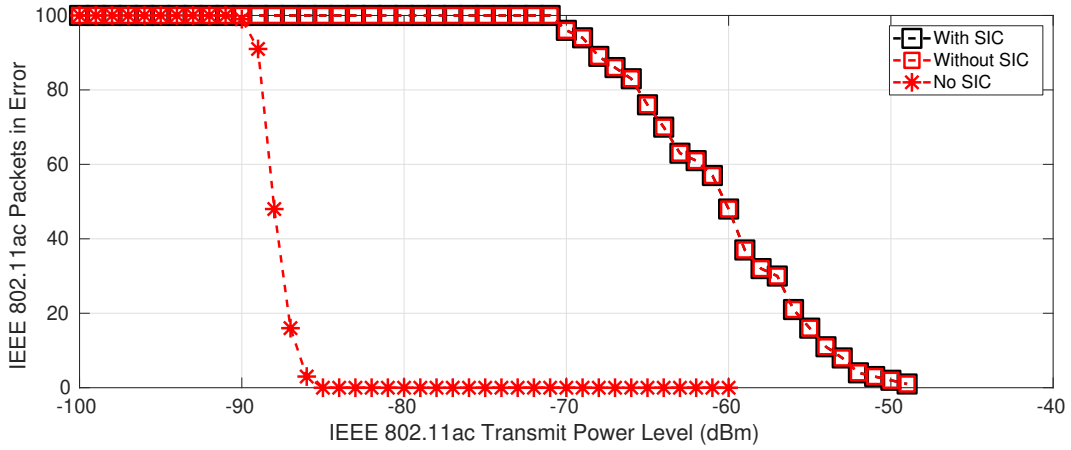


Fig. 5.11. Frame Error for IEEE 802.11ac MCS 4: With and Without Using SIC, LTE-LAA TxP −80 dBm

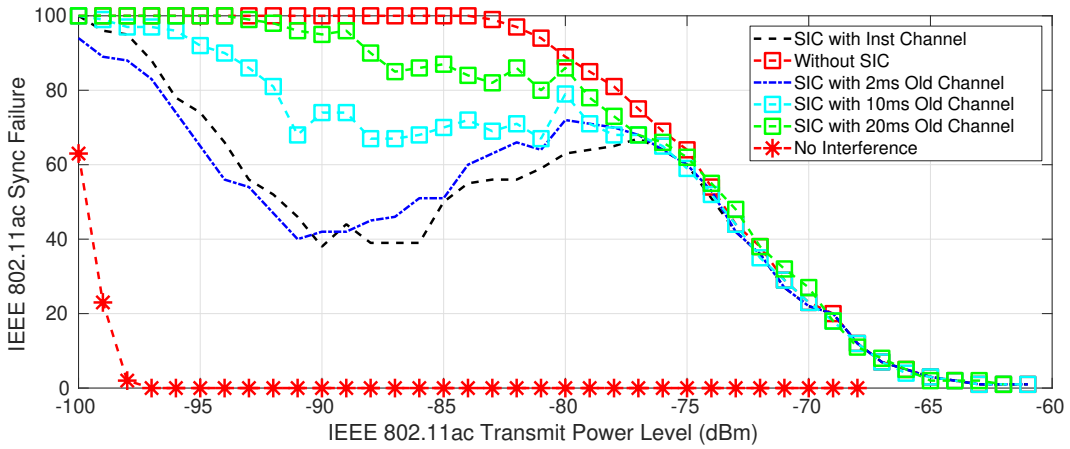


Fig. 5.12. Synchronization error of IEEE 802.11ac MCS 0 at inter frame arrival times 2 ms, 10 ms and 20 ms, LTE-LAA −80 dBm

5.2.3.2 Experiment-2: Comparison between SIC with Instantaneous Channel Estimates and SIC with Past Channel Estimates

With the same experimental settings as in Section 5.2.3.1, we simulate the interference between LTE-LAA and IEEE 802.11ac with inter frame intervals of $2, 10$ and 20ms. First we show the synchronization error plot corresponding to IEEE 802.11ac MCS 0 in Fig. 5.12. Observing the plot, we do not see any significant difference between SIC which uses old channel estimate taken 2ms before the collision and the SIC which uses instantaneous channel estimates except for marginal gain till −90 dBm. However, as we have seen in previous experiments, the performance of all types of SIC degrades as TxP of IEEE 802.11ac reaches near the TxP of LTE-LAA which is −80 dBm.

Next, we show the frame error plots when we use channel estimates from the past to perform SIC . Plots for IEEE 802.11ac MCS $0, 2$ and 4 are shown in Fig. 5.13, Fig. 5.14 and Fig. 5.15 respectively. We observe the following from the plots:

- Using old channel estimates notably reduces the frame errors, although cannot reduce the effect of interference completely.

- If the collision happens within 2ms, SIC using the old channel estimates provides significant advantage over SIC using instantaneous channel estimates.

- However, if the collision happens after 2ms, SIC using instantaneous channel estimates performs better.

- Likewise inthe previous cases, we see performance degrades as IEEE 802.11ac TxP reaches near the TxP of LTE-LAA which is −80 dBm.

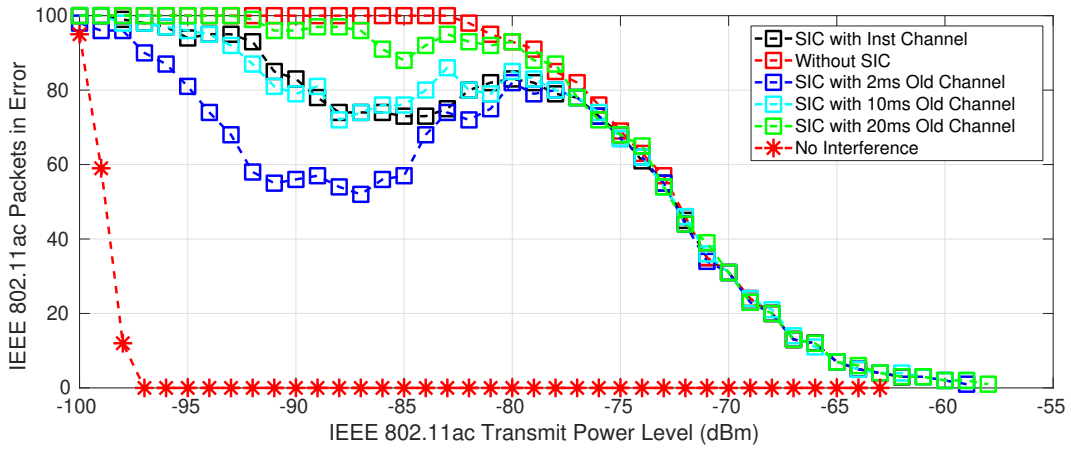


Fig. 5.13. Frame Error for IEEE 802.11ac MCS 0 at inter frame arrival times 2ms, 10ms and 20ms, LTE-LAA −80 dBm

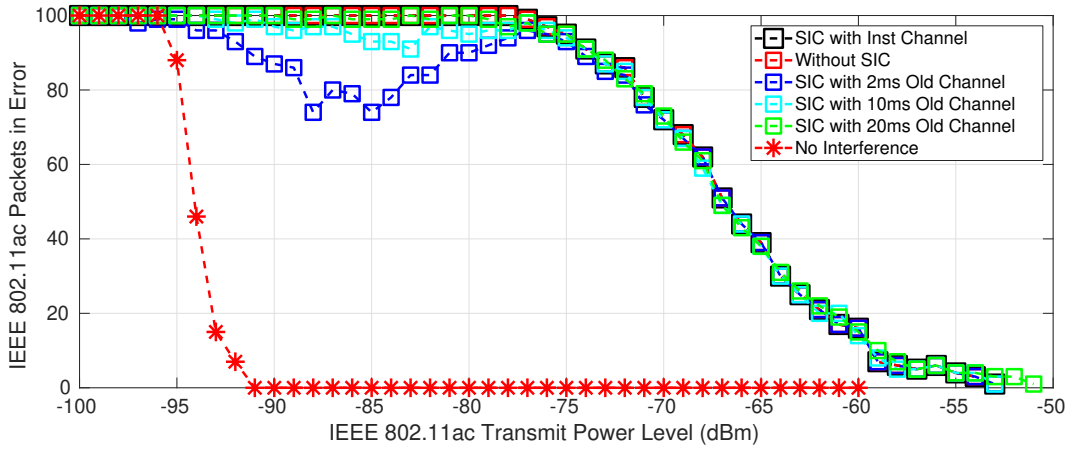


Fig. 5.14. Frame Error for IEEE 802.11ac MCS 2 at inter frame arrival times 2ms, 10ms and 20ms, LTE-LAA −80 dBm

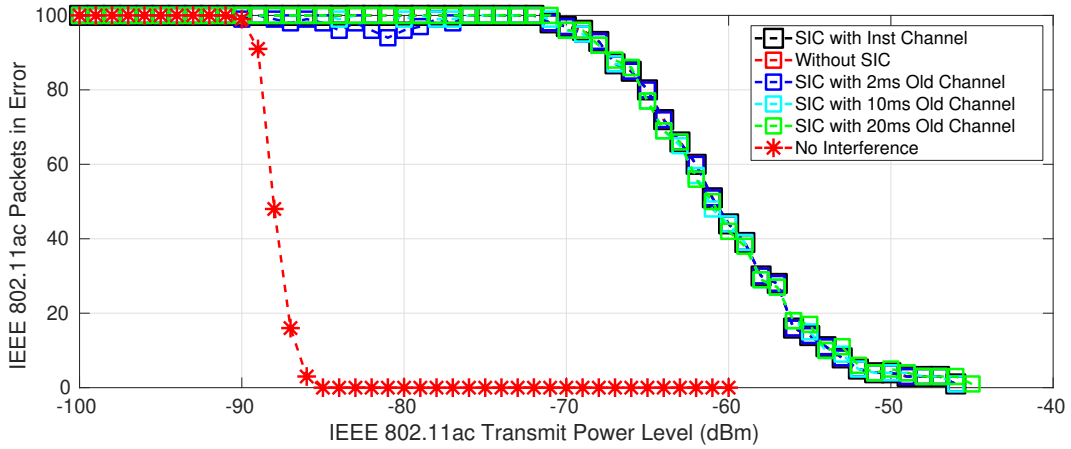


Fig. 5.15. Frame Error for IEEE 802.11ac MCS 4 at inter frame arrival times 2ms, 10ms and 20ms, LTE-LAA −80 dBm

5.2.4 Discussion

For a single antenna system, SIC is effective to mitigate the CCI. Not only it improves the performance, but also it is capable of recovering lost frames. In other words, it acts as a *re-synchronizing* receiver. Applying SIC using past channel estimates is beneficial inside an indoor environment which is characterized by a slow fading channel, i.e., low Doppler; however the inter-frame arrival time should be as low as 2ms. Besides, for any SIC to operate, the TxP of the weaker signal should be at least $5 - 10$dB less than the stronger signal.

5.3 Mitigating Interference in Multi-Antenna IEEE 802.11ac Receiver Caused by LTE-LAA

5.3.1 SIC of LTE-LAA from IEEE 802.11ac followed by MRC

From Section 4.5.4 and Section 4.7.1 we have learned that SIC of stronger signal followed by MRC of the weaker signal is capable of increasing the SINR of the weaker signal in a multi-antenna receiver. In this section, we attempt to apply the same concept for a multi-antenna IEEE 802.11ac receiver facing interference from LTE-LAA. Besides, to perform MRC, we apply implementation friendly Soft Bit Maximal Ratio Combiner (SBMRC) as discussed in Appendix B.2. Since the MATLAB receiver for IEEE 802.11ac uses Soft Decision Viterbi Decoder, implementing SBMRC becomes straightforward. Note that the operation of SBMRC followed by SIC does not have impact on the frame synchronization, hence we we chose frame CRC failures as our performance metrics in this experiment.

5.3.2 Simulations and Results

In this experiment, we have the same simulation parameters as in Section 5.2.3.1 except now the receiver has two antennas. Antenna correlation was chosen to 'Low' in the *MIMOCorrelation* parameter of the EPA channel model in MATLAB. We compare following methods in this experiment:

1. SBMRC[6] over the two antenna branches before SIC
2. SIC-SBMRC, i.e., SBMRC after SIC
3. SIC over single antenna with instantaneous channel estimates
4. SIC over single antenna with 2 ms old channel estimates
5. No SIC

Plots for IEEE 802.11ac MCS $0, 2$ and 4 are shown in Fig. 5.16, Fig. 5.17 and Fig. 5.18 respectively. From the plots we observe the following:

[6]We use MRC and SBMRC synonymously for this experiment

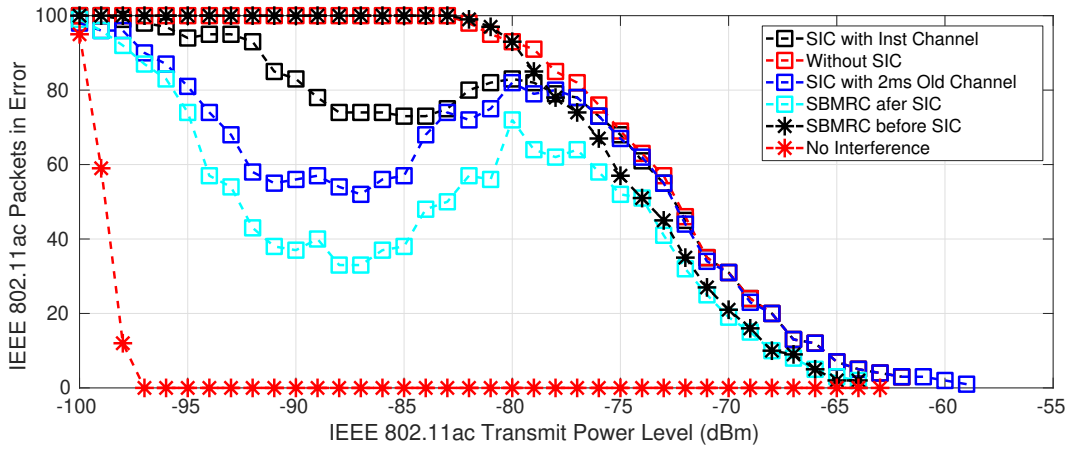


Fig. 5.16. Frame error for IEEE 802.11ac MCS 0: Performing SBMRC after SIC in a dual antenna receiver, LTE-LAA −80 dBm

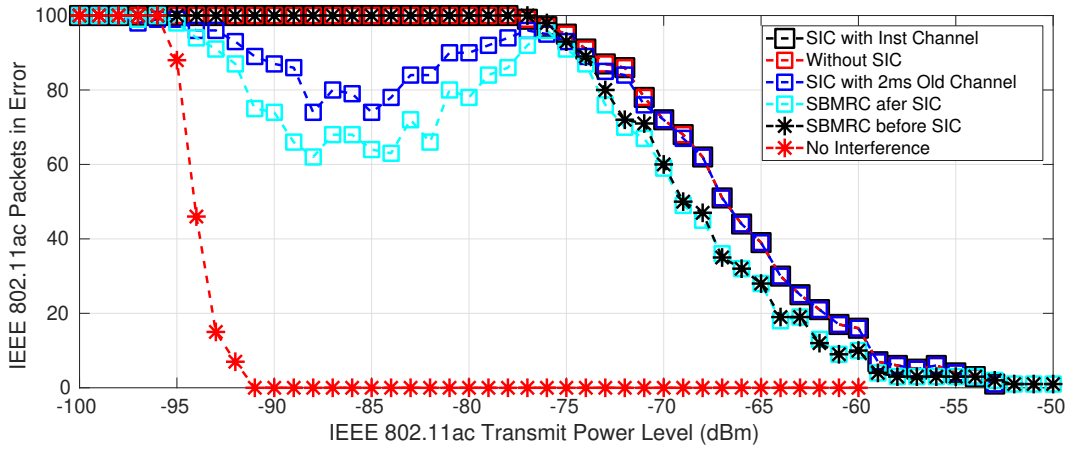


Fig. 5.17. Frame error for IEEE 802.11ac MCS 2: Performing SBMRC after SIC in a dual antenna receiver, LTE-LAA −80 dBm

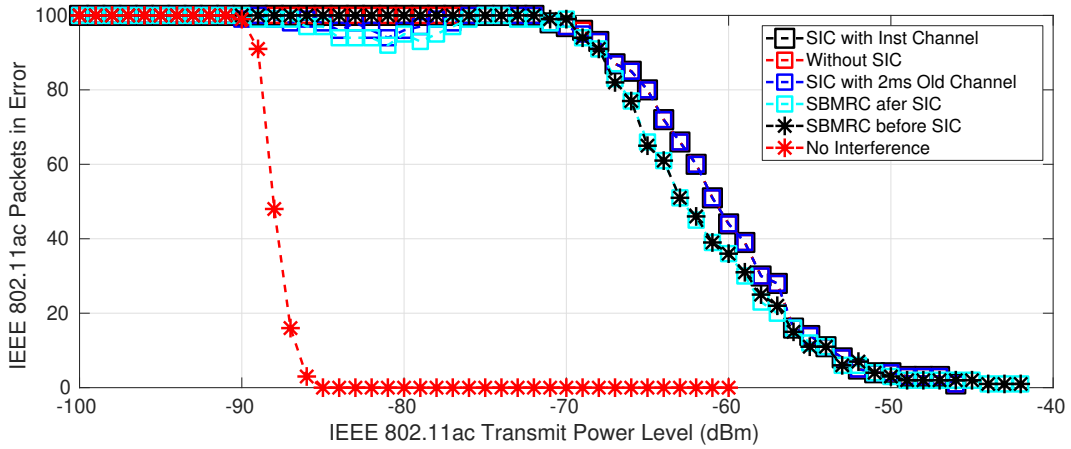


Fig. 5.18. Frame error for IEEE 802.11ac MCS 4: Performing SBMRC after SIC in a dual antenna receiver, LTE-LAA −80 dBm

- SIC-SBMRC outperforms SIC (both using old channels estimates and instantaneous channel estimates)
- At MCS greater than 0 where the SIC, either using instantaneous channel estimates or the past channel estimates, is unable to provide any performance gain; SIC-SBMRC provides notable gain. Although the gain fades away as the MCS increases with the reason being post-processing SINR after SIC-SBMRC not sufficient enough to decode the signals.

5.3.3 Discussion

SIC is an efficient method to mitigate CT-CCI, both in a single and multi-antenna receiver. SIC followed by SBMRC provides increased post-processing SINR for the weaker signal. However, SIC itself is a resource consuming process, and the computation power increases with the number of antenna branches over which SIC has to be performed. Besides, SBMRC followed by SIC requires LLR computation for all the antenna branches which could be resource consuming for higher MCS. Thus, although SIC followed by SBMRC provides notable gain, a trade-off between system complexity and performance has to be kept in mind while implementing the schemes on an SDR platform.

5.4 Summary of the Methods

We summarize the list of CT-CCI mitigation methods developed in this section in Table 5.2.

Table 5.2: Methods to Mitigate CT-CCI between two wideband OFDM signals

Interference Mitigation Method	**Interference Scenario**	**Number of Rx Antennas**	**Recovers**	**Re-Sync of weaker signal**	**Comments**
Successive Interference Cancellation of the stronger signal (SIC)	A strong wideband OFDM signal getting interfered by another $5-20$ dB weak wideband OFDM signal	1	Both the signals	Yes	
SIC of the stronger signal using old channel estimates	Same as above but under low mobility conditions	1	Both the signals	Yes	Suitable for low mobility environment only. In high mobility, its better to use instantaneous channel estimates
SIC of the stronger the signal followed by MRC of the weaker signal (SIC-MRC)	A strong signal getting interfered by a $5-20$ dB weak signal under low mobility conditions	2	Both the signals	Yes	Performing SIC on both branches followed by LLR computation could be complex, trade-off could be make between efficiency and available resources

5.5 Publications

- Kumar, Sumit; Kaltenberger, Florian; Ramirez, Alejandro; Kloiber, Bernhard: **A WiFi SIC Receiver in the presence of LTE-LAA for Indoor Deployment**. WCNC 2019, IEEE Wireless Communications and Networking Conference,15-18 April 2019, Marrakech, Morocco

Chapter 6

Simultaneously Decoding Heterogeneous Signals

In this chapter, we attempt to generalize the process of CT-CCI mitigation between any two given heterogeneous wireless standards. We start by developing decision trees to determine the simultaneous arrival of two heterogeneous wireless signals. Next, we design decision trees using the methods we have developed in previous chapters to mitigate CT-CCI between the two heterogeneous signals based on their physical layer characteristics.

6.1 Decision Tree: Interference Detection

In this section, we develop decision trees to detect the simultaneous arrival of two heterogeneous wireless signals. We start with the case of two known and heterogeneous wireless signals $S1$ and $S2$; both single antenna transmitters; whose physical layer characteristics, bandwidth, and frequency allocations are known beforehand. The receiver; which is also a single antenna; has the capability to decode both $S1$ and $S2$ simultaneously. Nonetheless, for both single antenna and multi-antenna receivers, the decision tree will be the same to detect the simultaneous arrival. We are not expecting any other collocated signal sharing its operating frequency band with $S1$ and $S2$. In other words, we expect reception of either $S1$ or $S2$ or both. Furthermore, both $S1$ and $S2$ are operating in interference limited region and not the noise-limited region.

A proposed decision tree, to be followed by the SMS-SDR to detect the simultaneous arrival of two heterogeneous wireless signals is shown in Fig. 6.1 with its continuation in Fig. 6.2. The receiver consists of two parallel receivers R_S1 and R_S2 responsible to detect and decode $S1$ and $S2$ respectively. During their course of operation, the receivers go through several states. The states of R_S1 are visible to R_S2 and vice versa. The decision tree is valid for any two heterogeneous signals $S1$ and $S2$ which are fully or partially overlapping each other in the frequency domain, irrespective of their physical layer characteristics. The very first step to receive $S1$ and $S2$ simultaneously is to perform

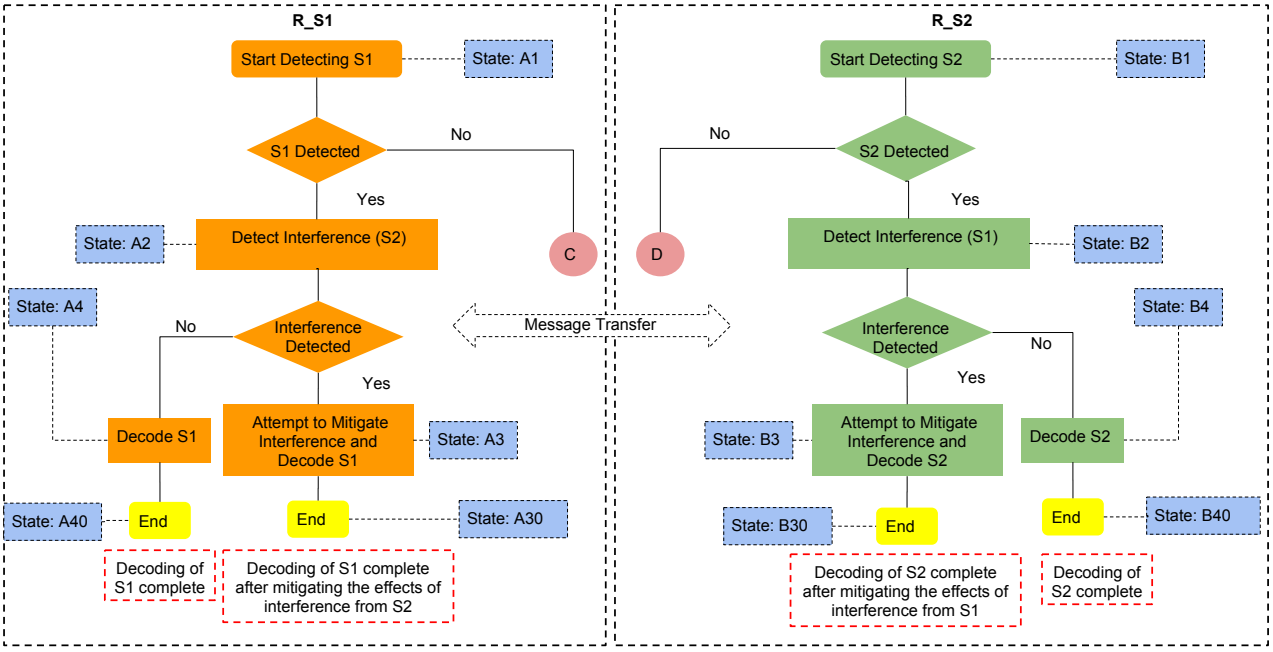


Fig. 6.1. Decision tree for the parallel receivers attempting to decode signals $S1$ and $S2$ simultaneously. The result after parsing the decision trees is either decoding the signals or detecting the interference. The figure continues to Fig. 6.2

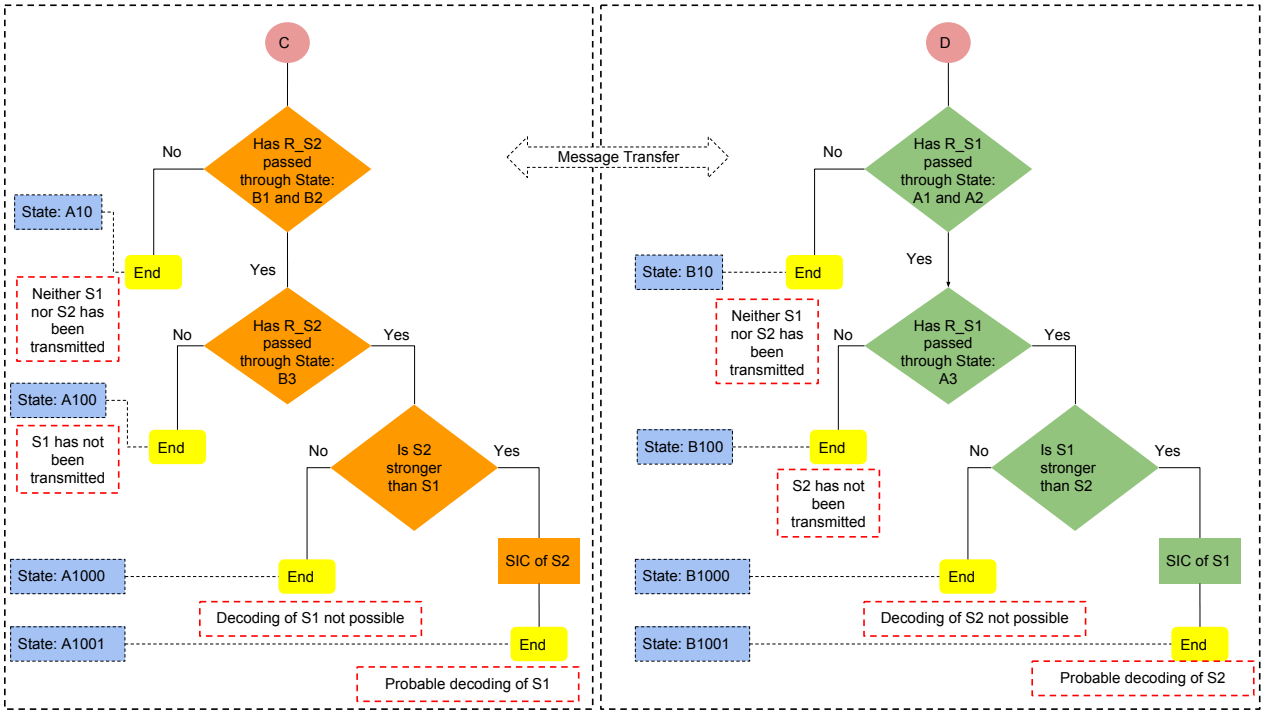


Fig. 6.2. Continuation of Fig. 6.1

channelization as discussed in Section 2.2.2; because in the beginning, the receiver does not know if $S1$ and $S2$ have arrived simultaneously, i.e., interference has occurred; and thus receiver attempts to decode both the signals $S1$ and $S2$. Without losing the generality, let us discuss the operational details of R_S1; nonetheless, the discussion is valid for R_S2. There could be the following three cases:

- **Case-1: $S1$ is detected and $S2$ is not detected**

  In this case, the operation is straightforward. $S1$ is decoded and in the process of decoding $S1$, an attempt is also made to detect the presence of $S2$, which could have been left undetectable due to collision with $S1$. Refer Section 6.1.1 and Table 4.5 for a summary of the interference detection methods. If $S1$ is detected, R_S1 attempts to mitigate the effect of interference and decode $S1$. In this case, the states R_S1 goes through are: **A1** $\rightarrow$ **A2** $\rightarrow$ **A3** $\rightarrow$ **A30**. In the other case R_S1 simple decodes $S1$ and terminates the operation. In this case, the states R_S1 goes through are: **A1** $\rightarrow$ **A2** $\rightarrow$ **A4** $\rightarrow$ **A40**.

- **Case-2: $S1$ is not detected and $S2$ is detected**

  This could happen due to two reasons: Either $S1$ is not transmitted at all or $S1$ is undetectable due to interference of $S2$. To find that, R_S1 attempts to look further. During the decoding of $S2$, R_S2 could detect the presence of $S1$ (if $S1$ was transmitted at all) and pass through the state $B3$. Thus R_S1 first looks if R_S2 has passed through $B3$.

  - If R_S2 has not passed through $B3$, that means $S1$ has not been transmitted or have been left completely undetectable due to interference of $S2$. At this point R_S1 terminates its operation. The states R_S1 has gone through are: **A1** $\rightarrow$ **A100**.
  - If R_S2 has passed through $B3$, then R_S1 can perform SIC of $S2$, depending on the power level difference between $S1$ and $S2$, to recover $S1$. If SIC is performed, the states R_S1 passes through are: **A1** $\rightarrow$ **A1001.**; however, if SIC is not performed, the states which R_S1 passes through are: **A1** $\rightarrow$ **A1000.**

- **Case-3: Both $S1$ and $S2$ are detected**

  In this case, R_S1 decodes $S1$ knowing that $S1$ has been subjected to interference by $S2$. Either the techniques to reduce the effects of interference can be applied during decoding of $S1$ or a re-synchronizing receiver can be used to clean $S1$ before the decoding. In this case, the states R_S1 goes through are: **A1** $\rightarrow$ **A2** $\rightarrow$ **A3** $\rightarrow$ **A30**.

At the end of the operation, R_S1 and R_S2 will be in the state of either completed the decoding of S1 and S2 respectively or waiting to be processed with CT-CCI mitigation methods to get detected and decoded.

6.1.1 Interference Detection

Before we start our discussion on the decision tree for CT-CCI mitigation, we briefly discuss the signal processing techniques required to detect the interference. As shown in Fig. 6.1, the states $A2$ and $B2$ correspond to detecting $S2$ by R_S1 and detecting $S1$ by R_S2 respectively. So, how do we apply our previous knowledge of interference detection given two heterogeneous wireless signals $S1$ and $S2$ whose physical layer characteristics and the frequency allocation is known beforehand. So far we have used two different methods of interference detection:

- **Noise Level Ratio based Interference Detection:**
  This method is discussed in Section 4.2.4. In an OFDM based system, the Localized Noise Variance Estimates can be computed, and the Noise Level Ratio (NLR) can be monitored to detect the presence of single and multiple narrowband co-channel interferers. The method is agnostic of the physical layer characteristics of the narrowband signal. Furthermore, the method is applicable when there is a partial overlap between an OFDM signal and another signal which is not necessarily OFDM or narrowband. A pictorial illustration of expected NLR for three possible cases in shown in Fig. 6.3. $S1$ is assumed to be OFDM while $S2$ can be OFDM or Non-OFDM. In case-(a), when $S2$ is narrowband compared to $S1$, the plot of NLR of $S1$ shows a distinguish lobe at the location of $S2$. Similarly, in case-(c) when $S2$ has comparable bandwidth compared to $S1$, and there is a partial overlap between $S1$ and $S2$, the plot of NLR of $S1$ shows a sudden rise at the edge where $S2$ start overlapping $S1$. However, in case-(b) when the bandwidths of $S1$ and $S2$ are comparable, the plot of NLR of $S1$ does not show distinguish lobes.

- **Error Vector Magnitude based Interference Detection:**
  NLR based interference detection requires at least one of the signals to be OFDM as well as no full overlap between the signal if they are of comparable bandwidths. To overcome these limitations, Error Vector Magnitude (EVM) between the received signal and regenerated signal can be monitored for a sudden jump. A sudden jump in the EVM could be an indicator of interference. Although a sudden jump in EVM could also be an indicator of deep fade, nonetheless, EVM based method is not limited by the physical layer characteristics of the signals and the extent of their overlap.

6.2 Decision Tree: Interference Mitigation

Once the simultaneous arrival of $S1$ and $S2$ has been confirmed, the next step is to mitigate the interference. In this section, we will use the CT-CCI mitigation methods developed in Chapter 4

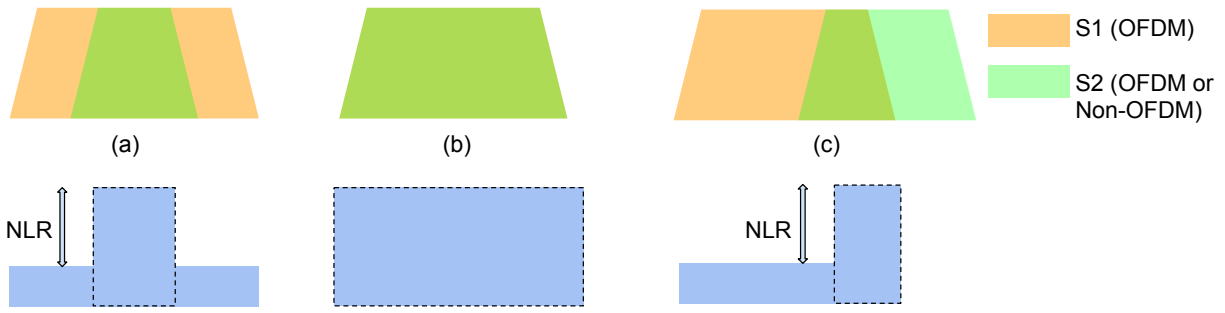


Fig. 6.3. Noise Level Ratio based interference detection in OFDM systems. Wideband OFDM can detect narrowband interference in case the interferer is narrowband as in (a) or there is a partial overlap as in (c). However it fails when both signals have comparable bandwidths as in (b)

and Chapter 5 to come up with a decision tree. The decision tree, on the basis of the physical layer characteristics of $S1$ and $S2$, will recommend the CT-CCI mitigation methods along with the required tailoring in the methods. As we have developed separate methods to mitigate CT-CCI in single and multi-antenna receivers, we will discuss them separately. We start with the single antenna receiver first.

6.2.1 Single Antenna Receiver

We consider three different cases for a single antenna receiver based on the signal characteristics:

1. **Interference between Wideband OFDM and Narrowband (OFDM or Non-OFDM) signals:**

   In this case, our objective is to recover both the wideband OFDM signal as well as the narrowband signal. Narrowband signal could be OFDM as well as non-OFDM. The proposed decision tree to recover the wideband OFDM signal is shown in Fig. 6.4(a). The receiver first decides if there is a partial or full overlap using NLR based interference detection method. In case of partial overlap, LNV-SC is performed over the overlapped subcarriers followed by soft-decision decoding. In case of full overlap, SIC is required to be performed which depends on the power level difference between the two signals. If the narrowband signal is sufficiently stronger (5-20 dB) than the OFDM signal, SIC of the narrowband signal is performed in order to recover the wideband OFDM signal. The operation is terminated if narrowband signal and wideband OFDM have comparable power levels. The proposed decision tree to recover the narrowband signal is shown in Fig. 6.4(b). First two decisions are made over whether the narrowband signal is OFDM or not, as well as if there is partial or full overlap between the narrowband signal and the wideband OFDM. By full overlap, we mean that the narrowband signal is fully contained inside the wideband signal as shown in Fig. 6.3(a). If the narrowband signal is OFDM and partially overlapped, LNV-Sc can be performed over the overlapped subcarriers. On the other hand, if the narrowband signal is fully overlapped or have a physical layer other than OFDM,

the SIC operation is required. However, the operation of SIC depends on the power level difference between the two signals and in this case if the power level of the wideband signal is sufficiently high (5-20 dB) compared to the narrowband signal, SIC can be performed to recover the narrowband signal. If not, the operation is terminated.

2. **Interference between two OFDM signals:**

   A proposed decision tree is shown in Fig. 6.5(a). The first decision is made whether both the signals are fully overlapped or partially overlapped. In case of partial overlap, LNV-Sc can be performed on both the OFDM signals over the overlapped subcarriers. In case of full overlap, SIC of the stronger OFDM signal is required to recover the weaker OFDM signal which in turn depends on the power level difference of the two OFDM signal. Failing to obtain the required power level difference, the operation is terminated after decoding the OFDM signal which has been detected. In all the cases, the operation is followed by soft-decision decoding which is more robust than hard decision decoding.

3. **Interference between two non-OFDM signals:**

   A proposed decision tree for this case is shown in Fig. 6.5(b). In this case, we rely entirely on the operation of SIC to recover both the signals. As the operation of SIC requires the power level of the stronger signal to be 5-20 dB higher than the weaker signal, this becomes the deciding factor in this case.

Although not indicated in the decision trees, wherever the indoor channel is available, the process to perform SIC using old channel estimates can be applied to make SIC more effective. Next, we discuss the decision trees developed for multi-antenna receivers Multi-antenna receivers provide a significant advantage over single antenna receivers especially in the case of CCI.

6.2.2 Multi-Antenna Receiver

Likewise the single antenna receiver, we consider three different cases for single antenna receiver based on the signal characteristics:

1. **Interference between Wideband OFDM and Narrowband (OFDM or Non-OFDM) signals:**

   A proposed decision tree for a multi-antenna receiver to recover the wideband OFDM signal is shown in Fig. 6.6(a). Unlike the single antenna case, now in the case of partial overlap three methods can be used which are MLSC, TIMO or DC-TIMO. All these methods are discussed in Chapter 4.

   Further, in the case of full overlap, the operation of SIC is required; however, in the multi-antenna case, SIC of the stronger signal can be followed by MRC over the weaker signal which

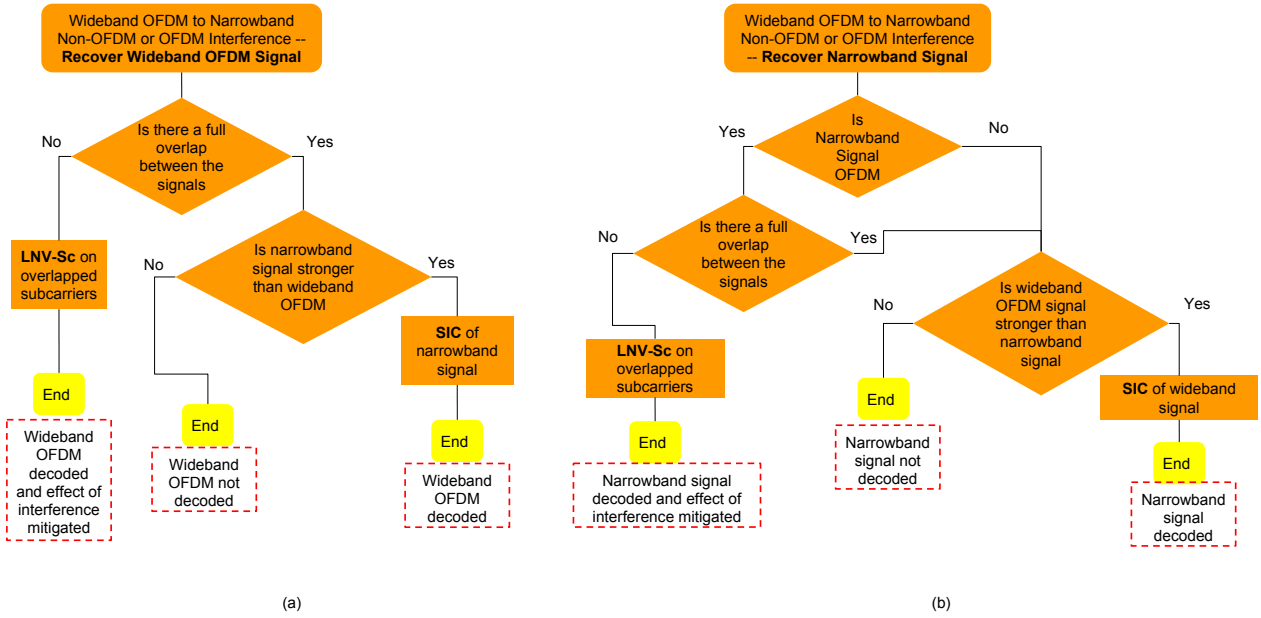


Fig. 6.4. (a) Decision tree to mitigate CT-CCI and recover wideband OFDM signal (b) Decision tree to mitigate CT-CCI and recover narrowband signal

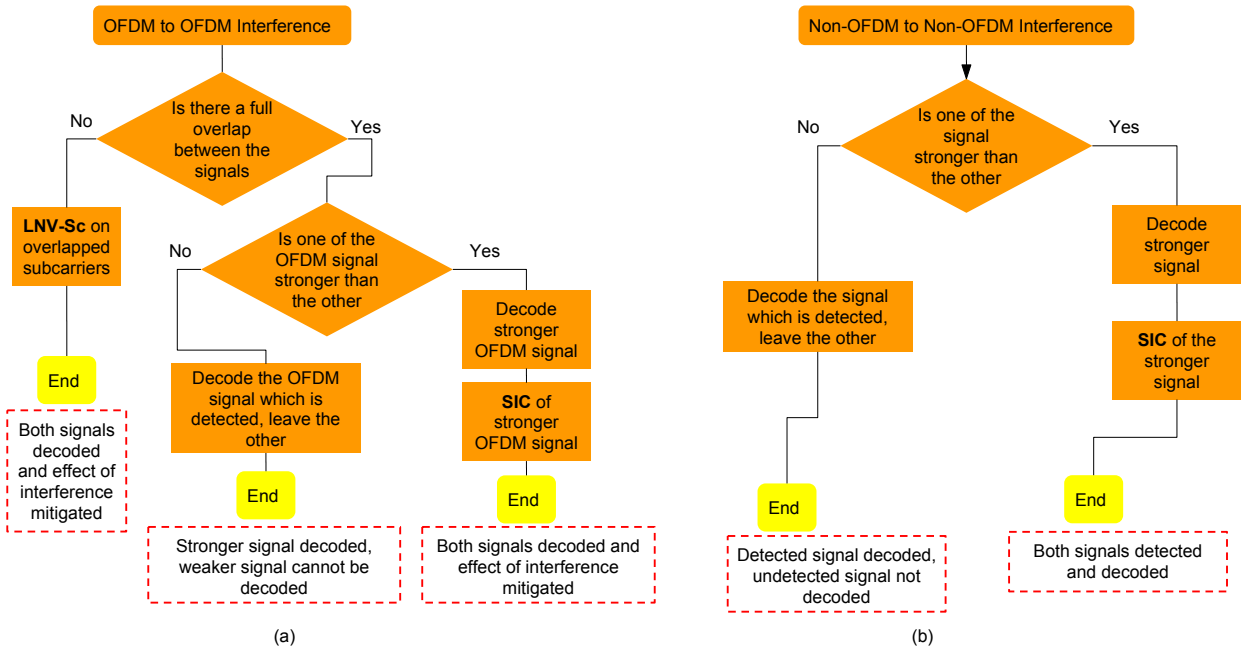


Fig. 6.5. (a) Decision tree to mitigate CT-CCI and recover OFDM signal in case of interference with another OFDM signal (b) Decision tree to mitigate CT-CCI and recover Non-OFDM signal in case of interference with another Non-OFDM signal

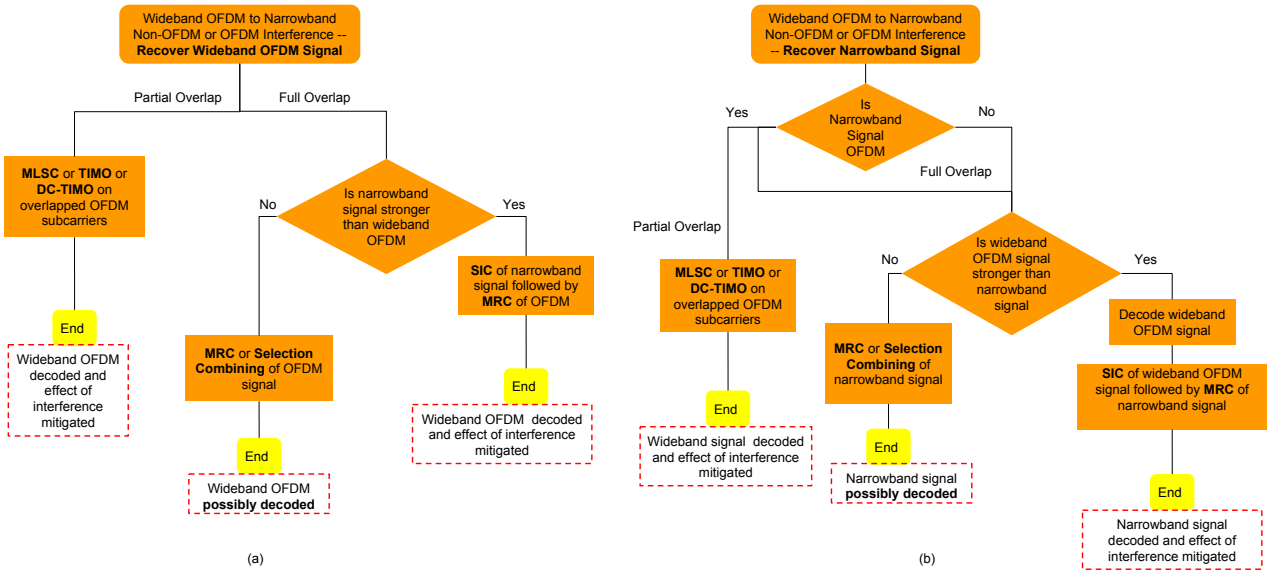


Fig. 6.6. (a) Decision tree to mitigate CT-CCI and recover wideband OFDM signal(b) Decision tree to mitigate CT-CCI and recover narrowband signal

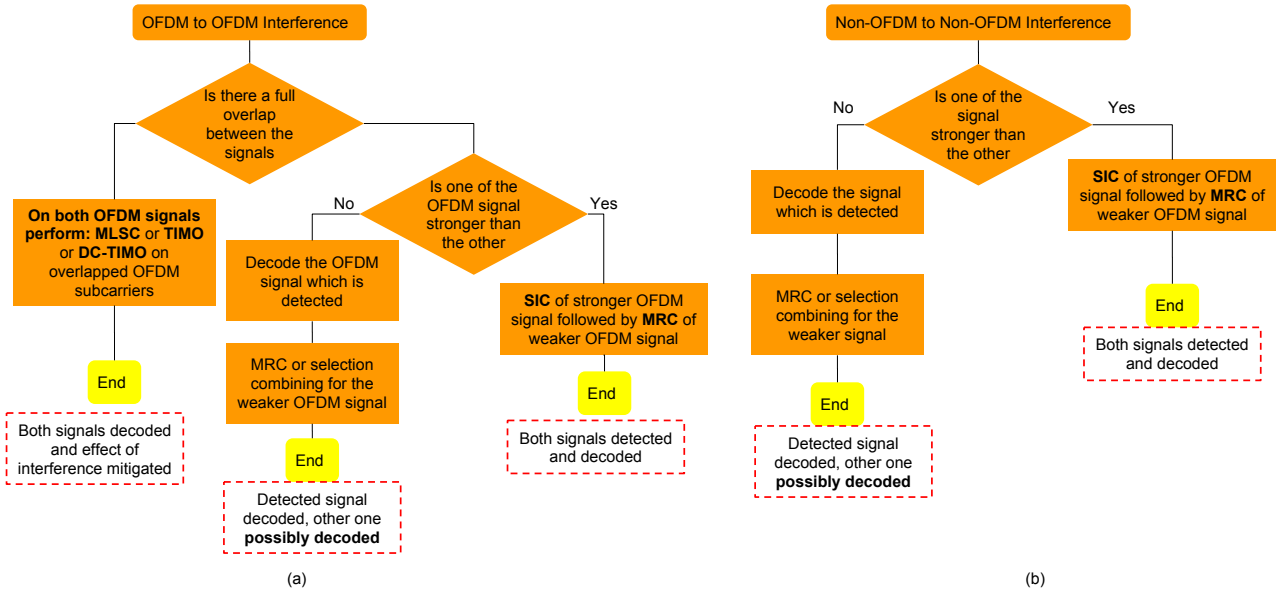


Fig. 6.7. (a) Decision tree to mitigate CT-CCI and recover OFDM signal facing interference from another OFDM signal (b) Decision tree to mitigate CT-CCI and recover a non-OFDM signal facing interference from another non-OFDM signal

gives a significant advantage over single antenna SIC. In addition, unlike the previous cases where the operation was terminated in case the required power level difference between the two signals was not attained, in a multi-antenna receiver, either MRC or Selection combining can be performed to get benefited from the diversity and mitigate CT-CCI.

The proposed decision tree to recover the narrowband signal is shown in Fig. 6.6(b). The decisions are made on the same parameters as in the single antenna case; however with multiple antennas, now the receiver can perform MLSC, TIMO and DC-TIMO to improve the performance. Additionally, the operation of SIC can be followed by MRC which gives a significant advantage over SIC on a single antenna. Finally, if the required power level to perform SIC is not obtained, an attempt can be made to recover the weaker signal by performing MRC or selection combining.

2. **Interference between two OFDM signals:**

   A proposed decision tree for this case is shown in Fig. 6.7(a). Likewise the single antenna case, the decision making parameters are same; however, now in the case of partial overlap MLSC, TIMO and DC-TIMO can be applied to both the OFDM signals. On the other hand, in the case of full overlap, SIC of the stronger OFDM signal can be followed by MRC of the weaker OFDM signal. In addition, if the requirements for SIC are not met, the stronger OFDM signal is decoded while MRC or selection combining is performed for the weaker signal if that is also detected.

3. **Interference between two non-OFDM signals:**

   A proposed decision tree for this case is shown in Fig. 6.7(b). Likewise the single antenna case, the decision is made over the same parameters; however, in order to recover the weaker signal, SIC of the stronger signal can be made more advantageous by performing MRC of the weaker signal after the SIC. Finally, unlike the single antenna case where the weaker signal has to be dropped in case the requirements to perform SIC are not met, with the multi-antenna receiver an attempt can be made to recover the weaker signal by performing MRC or selection combining before giving up.

Likewise, single antenna case, wherever there is an indoor channel, the method to perform SIC using old channel estimates can be readily applied make SIC more effective.

6.3 Discussion

In this chapter, first, we have developed and discussed decision trees to detect the interference, i.e., simultaneous arrival of the two signals of interest. After confirming the simultaneous arrival, we developed decision trees for mitigation of CT-CCI and attempted to recover both the signals. We

used the interference detection and interference mitigation methods developed in previous chapters. NLR based interference detection can provide instantaneous results; however, it requires the interferer to be either narrowband or partial interference in case the interferer has comparable bandwidth. On the other hand, EVM based interference detection can be used for all the cases, it may lead to false alarms as EVM can increase due to deep fades also.

Among interference mitigation methods, LNV-Sc is a promising method for OFDM based systems but, they require the interferers to be narrowband (in case of full overlap) or partial overlap in case the interferers are of comparable bandwidth. SIC is more effective compared to any other method; however, to perform SIC of the stronger signal, the weaker signal has to be 5-20 dB weaker which is not always possible to attain. Additionally, the performance of SIC is affected by the imperfection in channel estimates which is caused during CCI. In the case of indoor channels, the past channel estimates can be used to overcome such issues. Multi-antenna receivers give a significant advantage to SIC where MRC of the weaker signal follows after SIC of the stronger signal; however, the process adds more delay and complexity to the system.

Chapter 7

SDR Implementations

For the practical applicability of our methods and real-time verification of simulation results, we prototyped our methods in Software Defined Radio (SDR). In this chapter, we discuss the SDR implementations of particular methods from Chapter 4. We present the test set-up, experiments, and results of over-the-air (OTA) tests.

7.1 SDR Hardware and Software Tools

Our frequency of interest was 2.4 GHz ISM band, which has 80 MHz of usable bandwidth. Hence, for SDR hardware, we conducted an extensive survey of available SDR transceiver platforms for the frequency and bandwidth of our interest. The survey consists of state-of-the-art SDR platforms being used in academia as well as industry. It is presented in Table 7.1. We decided to chose Ettus USRP B210 as the hardware platform for our SDR because of the following criterion:

- Span of the bandwidth covers the wireless standards which we chose to work with, i.e., IEEE 802.11g, IEEE 802.15.4.
- Multiple B210 can be MIMO locked in order to process wider bandwidth.
- Previous experience with Ettus USRP devices.

On the software side, we used a combination of GNU Radio [6] and Openairinterface (OAI) [50]. Both GNU Radio and Openairinterface are academically popular SDR software tools and several implementations of wireless standards are readily available for experiments.

Now we discuss the implementations of selected algorithms which we have developed in the previous sections and the results of corresponding over-the-air testing.

Table 7.1: List of surveyed SDR Hardware Platforms

Manufacturer	**RF Front End**	**RF Bandwidth**	**RF Frequency Tuning Range**	**No. of Tx and Rx**	**ADC Rate(Bits)**	**DAC Rate(Bits)**
Ettus B210(Based on AD9361)	Inbuilt	56 MHz of realtime bandwidth (61.44MS/s quadrature)	70 MHz – 6 GHz	2 Tx/2 Rx	61.44(12)	61.44(12)
Ettus E310(Based on AD9361)	Inbuilt	56 MHz of realtime bandwidth (61.44MS/s quadrature)	70 MHz – 6 GHz	2 Tx/2 Rx	61.44(12)	61.44(12)
Blade RF (Based on LMS6002D)	Inbuilt	28 MHz	300 MHz – 3.8 GHz	1 Tx/1 Rx	40(12)	40(12)
Express MIMO 2(Based on 4 LMS6002D)	Inbuilt	28 MHz	300 MHz – 3.8 GHz	4 Tx/4 Rx	40(12)	40(12)
Noctar	Inbuilt	200 MHz	100 KHz – 4 GHz	1 Tx/1 Rx	125(12)	250(16)
Crimson	Inbuilt	1200 MHz	322 MHz – 6 GHz	4 Tx/4 Rx	370(16)	2500(16)
Myriad RF STREAM (LMS7002M)	Inbuilt	120 MHz	100 KHz – 3.8 GHz	2 Tx/2 Rx	160(12)	640(12)
Myriad RF NOVENA (LMS6002D)	Inbuilt	28 MHz	300 MHz – 3.8 GHz	1 Tx/1 Rx	40(12)	40(12)
Microsoft SORA	External	Maximum 40 MHz	Depends on the RF Front-end used	Depends on the RF Front-end used	NA	NA

7.2 LNV-SC

For this implementation, first, we developed a Soft-Decision IEEE 802.11g receiver using a combination of GNU Radio and Openairinterface. Both GNU Radio and Openairinterface contain standard compliant IEEE 802.11g receivers. Package available in GNU Radio, i.e., gr-ieee 802.11g contains Hard Decision Viterbi Decoder (HDVD) in the receiver. Hence, first, we changed the GNU Radio based receiver to output LLRs as we have to perform LLR scaling for all our single antenna interference mitigating methods. Next, we integrated Soft Decision Viterbi Decoder (SDVD) available in Openairinterface IEEE 802.11g receiver to decode the scaled LLRs outputted by GNU Radio. The output of the SDVD, i.e., bits are further processed using GNU Radio receiver blocks. The code has been made open source under GPL license and can be found [53].

7.3 SBMRC

Multi-antenna interference mitigation methods developed by us primarily use MRC. To implement MRC, we chose an implementation friendly way: Soft Bit Maximal Ratio Combiner(SBMRC). SBMRC combines the LLRs from individual antenna branches instead of complex samples. The theoretical details of SBMRC and its comparison with conventional MRC are given in Appendix B.2. Using our development of Soft Decision IEEE 802.11g receiver and SBMRC we further implemented Soft Bit Maximal Ratio Combiner with LLR Scaling (SB-MLSC). SB-MLSC is nothing but MLSC which uses SBMRC instead of MRC as the diversity combiner. A conventional MRC behaves as selection combiner when one of the antenna branches is not able to detect and decode frames. To replicate so, we added following functionalities in both SBMRC and SB-MLSC:

- Combining of the LLRs from both antenna branches happens if and only if:
  - Frame is detected on both the antenna branches
  - SIGNAL field passes the parity check on both the antenna branches
- If any of the antenna branches fail to detect WiFi frame or the SIGNAl field parity check fails, the SBMRC starts tracking the antenna branch where both frame detection and SIGNAL parity check is successful. In other words, SBMRC operates as a selection combiner if one antenna branch fails to detect and/or decode packets.

A block diagram of SB-MLSC is shown in Fig. 7.1. Soft Decision IEEE 802.11g receiver [53] developed by us can be easily configured to output LLRs and adding the LLRs from two antenna branches is a trivial task in GNU Radio. Hence the implementation of SBMRC and SB-MLSC is significantly simplified.

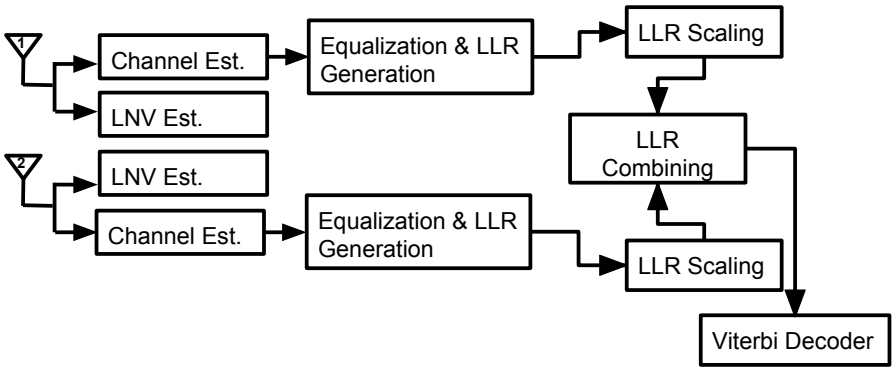


Fig. 7.1. Soft Bit Maximal Ratio Combiner with LLR Scaling

Table 7.2: List of Hardware for OTA tests of LNV-SC, SBMRC and SB-MLSC

SDR Hardware	Ettus USRP B210
SDR Software	GNU Radio Ver 3.7.1, Openairinterface, UHD 3.11
RF Cage	Ramsey STE 2200
Antenna	VERT2450 Vertical Antenna (2.ncy of interest was vvvv4-2.5 and 4.9-5.9 GHz) Dualband
CPU	Dell Precision 5510, Gigabyte BRIX PC

7.4 OTA Testing: Test Set-Up, Experiments, and Results

The test set-up of OTA testing is shown in Section 7.4. It consists of a dual-technology USRP B210 transmitter capable of transmitting both IEEE 802.11g and ZigBee frames simultaneously. Before transmission, we perform time alignment of IEEE 802.11g and ZigBee frames to create 100% chance of a collision which replicates our simulation scenario. The frame parameters of WiFi and ZigBee are the same as mentioned in Table 4.1; however, now the transmission happens over a physical channel. We have used RF cage for all our experiments to avoid interference from ambient IEEE 802.11g transmissions. For the proof of concept, we have used only IEEE 802.11g MCS 0 for our all the OTA experiments. Besides, GNU Radio provides tuning the transmit power of USRP using normalized transmit gain instead of the absolute value of gain. Hence, for all the OTA experiments, we have used normalized transmit gain values which are direct indicators of the Transmit Power Level(TxP). For a given TXP of IEEE 802.11g and ZigBee, we repeat the same experiment 4 times. Each trial of the experiment consists of transmitting a fixed number of IEEE 802.11g frames and logging the percentage of the received frames which pass the CRC test. Finally, an average is taken for plotting the results. A brief schematic of the test set-up is also shown in Fig. 7.2 with the list of hardware used are tabulated in Table 7.2.

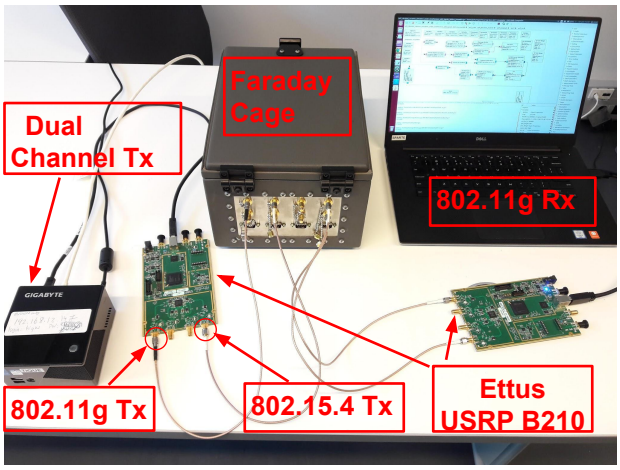


Fig. 7.2. Over-the-air test set-Up: USRP B210, RF Cage and General Purpose CPU

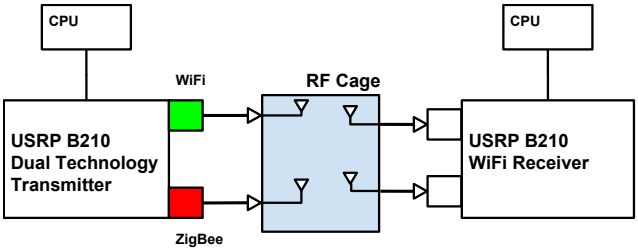


Fig. 7.3. Over-the-air Test Schematic corresponding to Section 7.4

Experiment-1: LNV Estimation and LLR Scaling (LNV-SC) in Single Antenna IEEE 802.11g Receiver in the presence of One ZigBee Interferer

In our first experiment, we replicate the simulation experiment as in Section 4.2.5.1 where a single ZigBee interferer causes the interference. We used two fixed value of interferer's normalized transmit gain (0.01 and 0.05) and varied IEEE 802.11g frame's normalized transmit gain from 0.0 till all the transmitted IEEE 802.11g frames were correctly received. As a performance metrics, we chose % of packets received by each method for a given normalized transmit gain of IEEE 802.11g transmitter.

Experiment-2: LNV Estimation and LLR Scaling (LNV-SC) in Single Antenna IEEE 802.11g Receiver in the presence of Two ZigBee Interferers

In this experiment, we perform the same experiment as in Section 7.4, but now the interference is caused by two ZigBee interferers. We used two fixed value of interferer's normalized transmit gain (0.01 and 0.05) and varied IEEE 802.11g frame's normalized transmit gain from 0.0 till all the transmitted IEEE 802.11g frames were correctly received. As a performance metrics, we chose % of packets received by each method for a given normalized transmit gain of IEEE 802.11g transmitter.

Experiment-3: SB-MLSC for two antenna IEEE 802.11g Receiver in the presence of One ZigBee Interferer

In this experiment, we attempt to replicate the simulation experiment as in Section 4.5.4. OTA testing of SB-MLSC was tricky because it has to be done inside an RF cage where multi-paths are not possible due to thick absorbent layer inside it. Also, inside the RF cage where antennas are placed nearby, the strength of interference on all the antenna branches are nearly equal, and hence the effect is the same. The idea behind exploiting multi-paths is that once interference arrives via different paths, its strength is different on the different antennas of the receiver. CCI on IEEE 802.11g packets obtained from any of the receive antenna branches depends on the extent of interference on that antenna branch. Knowing that the ultimate effect due to CCI on WiFi packet is CRC fail, we decided to improvise our test methodology by manually emulating the CCI effect. We decreased the strength of IEEE 802.11g signal on one of the antenna branches by partially/fully covering one of the receive antenna branches using aluminum foils. As the previous two experiments already showcased the effectiveness of our interference mitigation methods, we limit our scope in this experiment to the verification of operational and tracking capabilities of SB-MLSC. We analyzed the following three cases during this experiment.

- **Case-1:** Partially covering one of the receive antenna branches: This reduces the IEEE 802.11g signal strength on that antenna branch.
- **Case-2:** Fully covering one of the receive antenna branches with aluminum foil: This nulls the IEEE 802.11g signal strength on that antenna branch.
- **Case-3:** Placing scrambled aluminum foils inside the RF cage: This was done in an attempt to emulate multi-path reflections inside the RF cage.

Results and Discussion

Experiment-1

The bar chart for this experiment is shown in Fig. 7.4. First of all, we observe that due to ZigBee interference the % of received IEEE 802.11g packets (which pass the CRC test) severely degrades. For example, the bars corresponding to LNV-SC and Conv-SC lags behind the blue bars (W/o means without). This result agrees with our simulation results. We observe this degradation for both ZigBee normalized transmit gain of 0.01 and 0.05. Next, we observe that for a given % of received IEEE 802.11g packets, performing LLR scaling with LNV (Proposed method LNV-SC) significantly reduces the transmit power requirement compared to the conventional method (Conv-SC). For example, for interferer's normalized transmit gain of 0.05, the green bars lag behind the violet bars. As expected, as

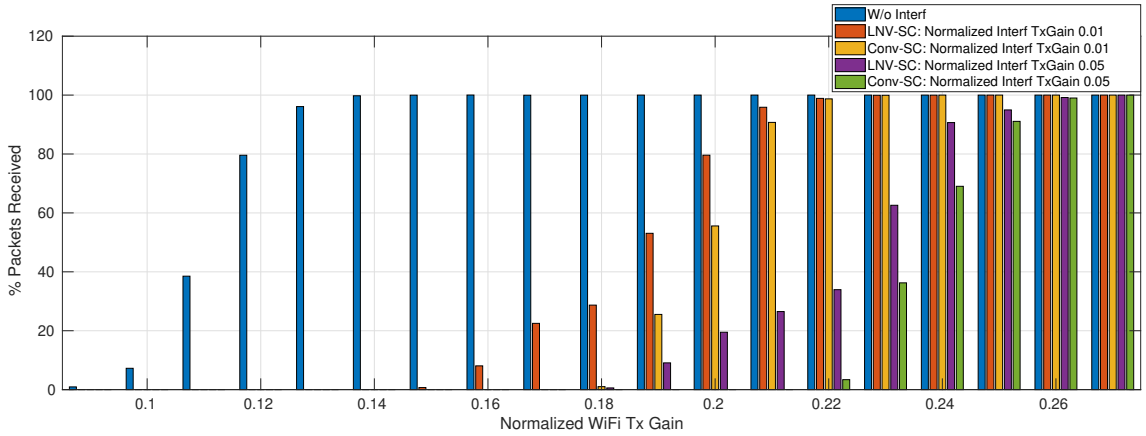


Fig. 7.4. LNV-SC (proposed method) in the single interferer case leads to more IEEE 802.11g frames passing CRC test compared to Conv-SC (conventional method) at a lower IEEE 802.11g TXP. This is observed for both the experimented interferer TXP

the normalized transmit gain of IEEE 802.11g is increased, IEEE 802.11g dominates over interference, and both the methods show the same performance.

Experiment-2

The bar chart for this test is shown in Fig. 7.5. Similar to the previous experiment-1, we observe that due to ZigBee interference the % of received IEEE 802.11g packets (which pass the CRC test) severely decreases. However, the performance degradation is more compared to the single interferer case. For example, the orange bars in Fig. 7.5 lag behind the orange bars in Fig. 7.4. This also agrees with our simulation results. We observe this for both the ZigBee normalized transmit gain of 0.01 and 0.05. Next, just like experiment-1, we observe that for a given % of received IEEE 802.11g packets, performing LLR scaling with LNV (LNV-SC) reduces the transmit power requirement significantly compared to the conventional method (Conv-SC). For example, for interferer's normalized transmit gain of 0.05, the green bars lag behind the violet bars. As expected, as the normalized transmit gain of IEEE 802.11g is increased, IEEE 802.11g dominates over interference, and both the methods show the same performance.

Experiment-3

We present three different sets of results corresponding to the three cases discussed in Section 7.4.

1. The results corresponding to the case-1 are plotted in Fig. 7.6. We performed 3 trials of the experiment (with different interference TXP) wherein each we partially covered the receive antenna branch 2 with aluminum foil which resulted in SB-MLSC tracking the branch 1 which was stronger.

2. The results corresponding to the case-2 are plotted in Fig. 7.7. We performed 3 trials of the experiment (with different interference TXP) where we completely covered the receive antenna

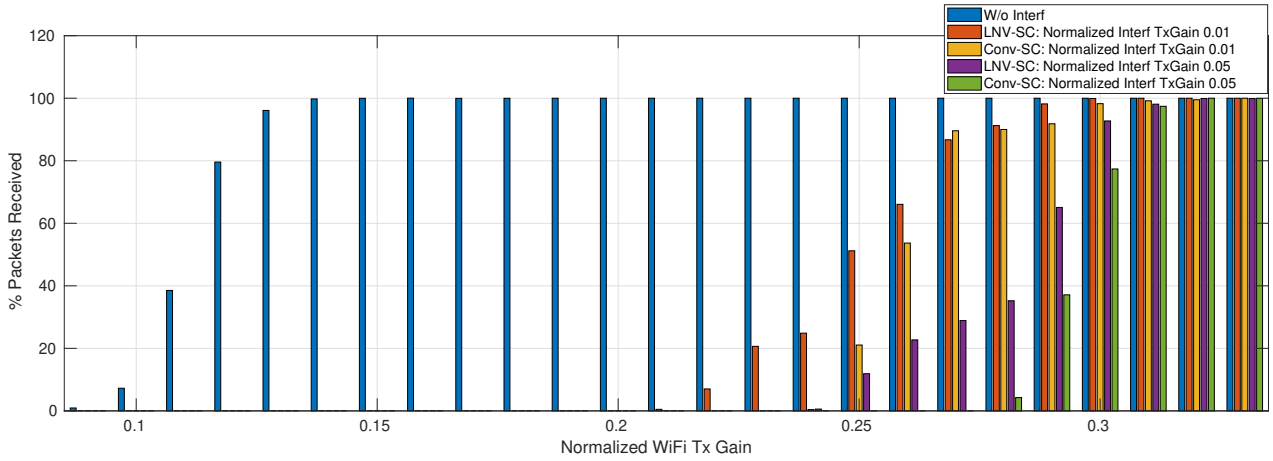


Fig. 7.5. LNV-SC (proposed method) in the two interferer case also leads to more IEEE 802.11g frames passing CRC test compared to Conv-SC (conventional method) at a lower IEEE 802.11g TXP. This is observed for both the experimented interferer TXP

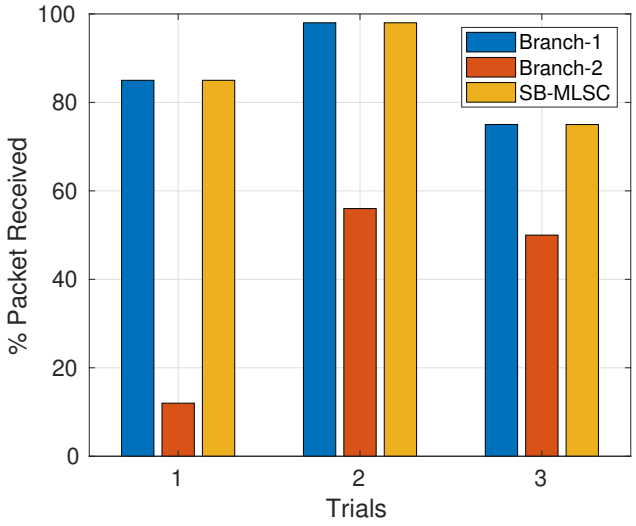


Fig. 7.6. Branch-2 is partially covered with aluminum foil thus, receives lesser packets than Branch-1. In this case, SB-MLSC tracks Branch-1 which receives more packet than Branch-2.

branch-1 with aluminum foil which effectively stopped branch-1 from receiving any IEEE 802.11g frame. This resulted in SB-MLSC receiving the same number of IEEE 802.11g packets as antenna branch-2, i.e., SB-MLSC again tracked the stronger branch and behaved as a selection combiner.

3. The results corresponding to the case-3 are plotted in Fig. 7.8. We placed scrambled aluminum foils inside the RF cage to emulate multi-path reflections. We performed 3 trials of the experiment where we changed the positions of aluminum foils inside the RF cage. We indeed observe diversity gain for several placement scenarios of the scrambled aluminum foil although the gain was marginal.

Results corresponding to all the three cases of Experiment - 3 indicate the proper operation and tracking capability of SB-MLSC.

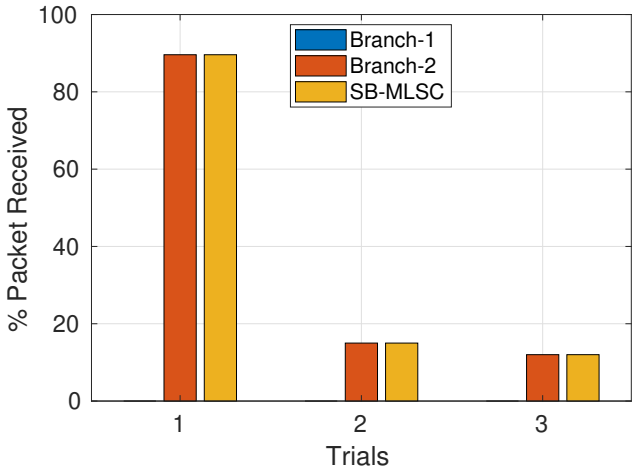


Fig. 7.7. Branch-1 is fully covered with aluminum foil and hence ceases to receive any packet. In this case, SB-MLSC tracks Branch-2 when Branch-1 is killed.

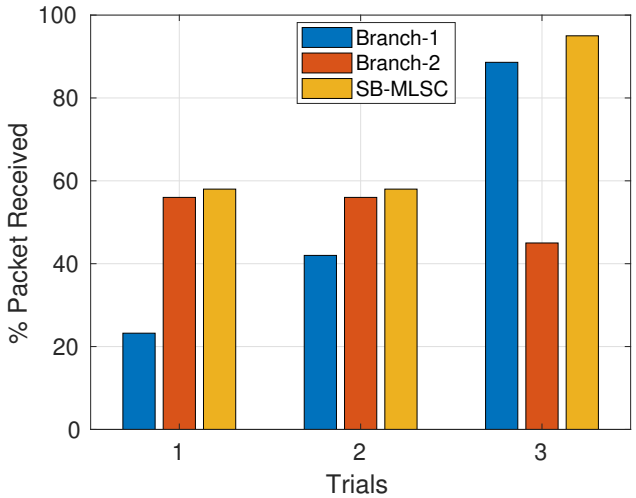


Fig. 7.8. Scrambled aluminum foils are placed inside RF cage resulting in multi-apth reflections. In this case, SB-MLSC provides diversity gain, i.e., receives more packet than both Branch-1 and Branch-2.

7.5 ZigBee Double Receiver

While implementing MRC for ZigBee, it was found that *Double Receiver* [12, Sec 4.4.1] performs as good as MRC for ZigBee. The architecture of the double receiver is straightforward and reduced our time of prototyping and testing. In a double receiver, signals are collected and decoded from all the antenna branches and finally sorted and merged. This is unlike the selection combining where only one branch is decoded at a time, and rest are ignored. In a double receiver, signals from all the branches are preserved. The implementation simplicity of double receiver motivated us to implement it in GNU Radio directly and perform quick over-the-air testing.

To experience diversity, i.e., independent fading, the minimum distance between the two antennas of the receiver should be $\lambda/2$ where λ is the wavelength. This minimum distance is 6.25cm at 2.4 GHz. USRP B210 has two receiver ports the distance between them is approx 6 cm. Hence, USRP B210 is suitable to exploit independent fading. A block diagram of the ZigBee Double receiver developed by us in GNU Radio is shown in Fig. 7.9. Individual ZigBee receivers decode the same samples, and the

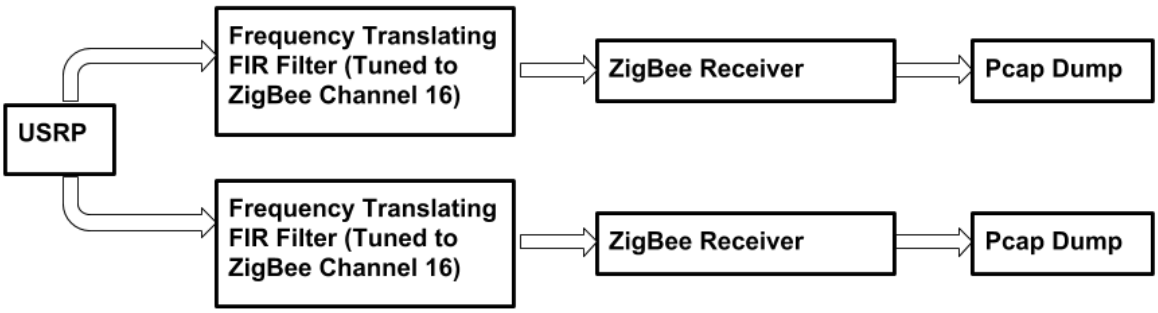


Fig. 7.9. GNU Radio Schematic For Double Receiver. The receiver is tuned to ZigBee channel-16 in 2.4GHz ISM band. A double receiver operates by decoding all the branches simultaneously. This is contrast to selection combiner which selects one out of many available branches.

packets which pass the CRC are dumped in .pcap files for further analysis.

OTA Testing: Test Set-Up, Experiments, and Results

The double receiver was tested at Eurecom against commercial ZigBee transmitter. At Eurecom, there are at least $3-4$ WiFi access point operating on channel-6 which also overlaps with ZigBee channel16 and channel-17. Hence the scenario at Eurecom is sufficient enough to provide CCI for ZigBee. Test specifications are mentioned in Table 7.3. Received packet count from both the antennas of the double receiver were compared for every 1000 packet sent from the transmitter. We conducted tests for 4 different normalized gains values of receiver. Results are shown in Fig. 7.10a, Fig. 7.10b, Fig. 7.10c, and Fig. 7.10d corresponding to normalized receiver gain values of 0.3, 0.4, 0.5 and 0.6 respectively. We observe that per 1000 packets sent by the transmitter, the two antenna branches show a significant

Table 7.3: Hardware used for OTA Tests of ZigBee Double Receiver

ZigBee Transmitter	Digikey XBee Pro
ZigBee Channels	Ch-16(2.430 GHz)
Distance between Tx and Rx	∼35 Meters
Normalized Receiver Gain	$0.3, 0.4, 0.5, 0.6$
ZigBee Tx Power	10 dBm
ZigBee Double Receiver	NI USRP-2901

difference in the number of packets received. We also observe that the difference is very prominent at lower values of double receiver gain. Further, the received packets can then be sorted and merged to get the correct packets in sequence.

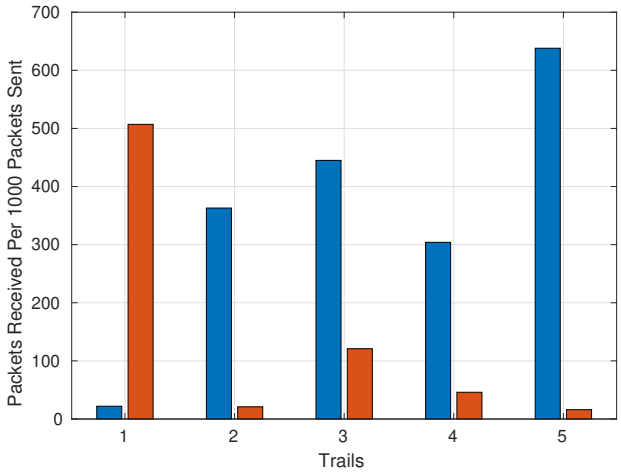
7.6 Filter Bank Channelizer

An important task to receive multiple wireless signals facing CCI is to separate the signals before the baseband signal processing starts. We take the case of IEEE 802.11g and ZigBee where within one IEEE 802.11g 20 MHz wide channel there could be 4 ZigBee channels each 2 MHz wide. Their sampling rates are respectively 20MHz and 2MHz. We aim to carve out single narrowband ZigBee channel embedded inside the 20 MHz spectrum chunk obtained at a sampling rate of 20 MHz. There are three steps in this process: Bandpass filtering, Center Frequency Translation, and Resampling. We combined all the three steps into one single steps using GNU Radio.

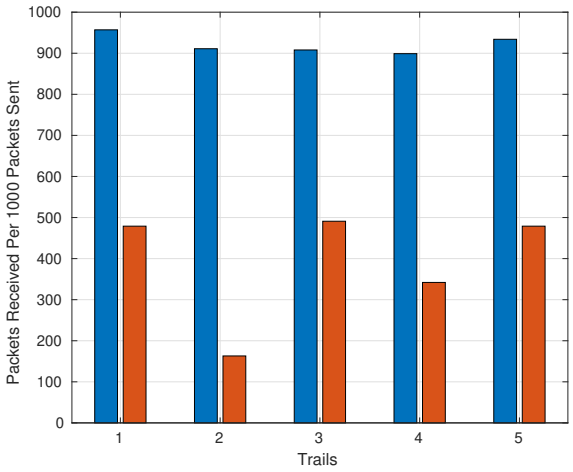
In general, to receive a narrowband signal N with sampling rate X MHz and center frequency A GHz from wideband signal M with sampling rate Y MHz and center frequency B GHz, where $Y > X$ and $B + (Y/2) \geq A \geq B - (Y/2)$ Following steps are required:

1. Sample at Y MHz with center frequency at B GHz
2. Frequency translation to the center frequency of X i.e. A GHz
3. Anti-aliasing filtering $-Y/(2 * \text{decimation rate})$ to $Y/(2 * \text{decimation rate})$
4. Decimate by Y/X to get X MHz of signal N
5. Feed to receiver of N
6. Meanwhile the sampled data at Y MHz centered at B GHz can be fed to the receiver of M.

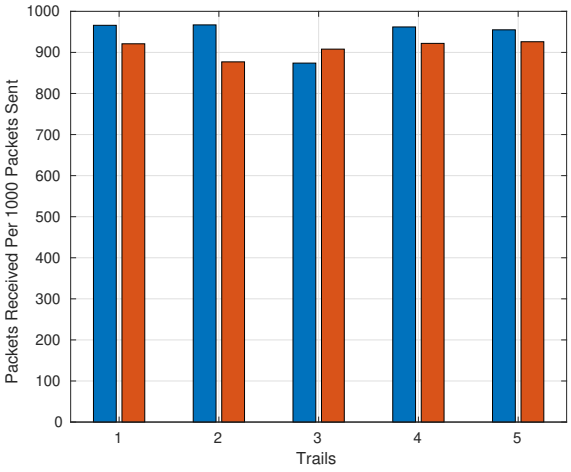
The process is illustrated in Fig. 7.11. GNU Radio block named **Frequency Xlating Filter** does all the tasks by taking the appropriate parameters as shown in Fig. 7.12. Center_offset is the parameter which decides the frequency translation from the center frequency. An important part is filter design and setting the transition bandwidth of low pass anti aliasing filter.



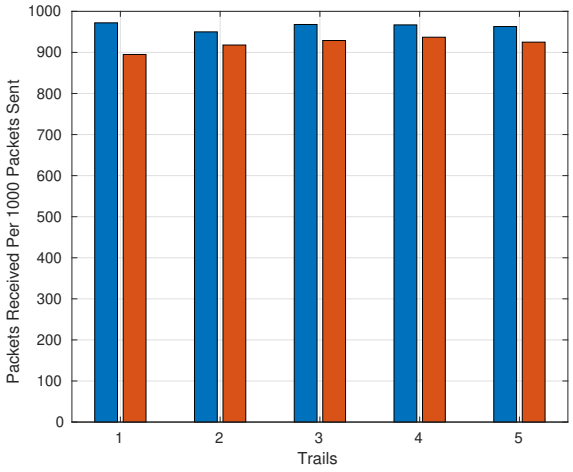
(a) Normalized Rx Gain 0.3



(b) Normalized Rx Gain 0.4



(c) Normalized Rx Gain 0.5



(d) Normalized Rx Gain 0.6

Fig. 7.10. Performance of ZigBee double receiver under several normalized receiver gain. As the gain increases, both the antenna branches show similar performance. The experiment shows that diversity based reception show better performance when the system operate at the boundary of noise limited region.

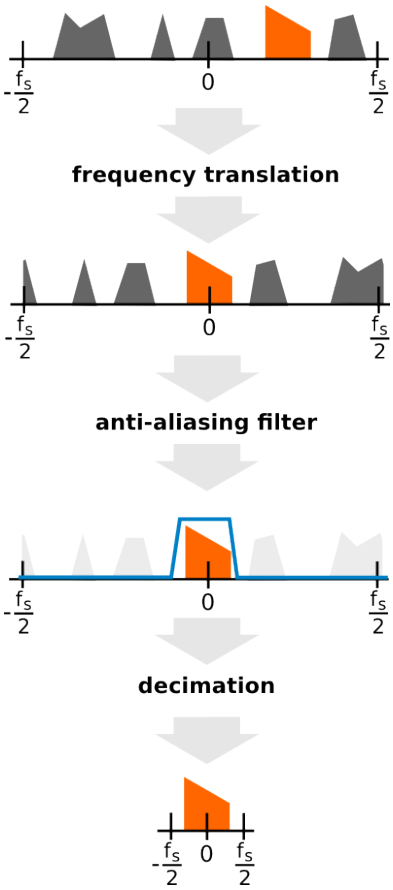


Fig. 7.11. Functionality of a basic spectrum carving module for SMS-SDR. We have used spectrum carving and channelizing synonymously in this thesis.

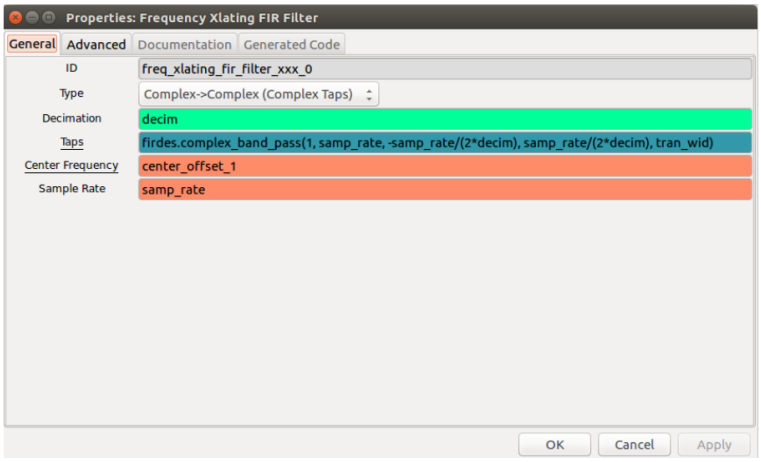


Fig. 7.12. GUI of GNU Radio FreqXlating Filter Options. The block can be configured to perform frequency translation and decimation (if required) simultaneously.

OTA Testing: Test Set-Up, Experiments, and Results

Using the method above a ZigBee receiver was configured to receive 2 ZigBee streams at channel-16(2.430 GHz) and channel-19(2.445GHz). Both of these ZigBee channels are overlapped by IEEE 802.11g channel-6 which is centered at 2.437 GHz. Hardware used for this experiment is listed in Table 7.3. GNU Radio Frequency Xlating Filter provides two different methods to implement the filters: FIR filters and FFT based filters: We used both of them and varied the transition width of the filters. With our experiments we found that:

- A transition width of 500 KHz is free of overruns. Below that both FIR and FFT based Channelizer shows overruns.
- Number of filter taps needed for FIR based Channelizer is significantly larger than FFT based Channelizer. A higher number of filter taps consumes more CPU during over the operation leading to overruns warning from the UHD.
- At a transition width of 500 KHz, out of 1000 transmitted packets, the receiver using FIR based Channelizer collects only 4 packets which pass CRC check while it was 996 for the receiver which used FFT based Channelizer.

7.7 Demonstrations

- Kumar, Sumit; Kaltenberger, Florian: **SDR implementation of narrow-band interference mitigation in wide-band OFDM systems** SPAWC 2018, 19th IEEE International Workshop on Signal Processing Advances in Wireless Communications, 25-28 June 2018, Kalamata, Greece
- Kumit, Sumar; Kaltenberger, Florian: **Mitigating multiple narrowband interferers in SDR IEEE 802.11g diversity receiver** ACM MobiCom 2018, 24th Annual International Conference on Mobile Computing and Networking, 29 October-2 November 2018, New Delhi, India

Chapter 8

Conclusions and Future Research

8.1 Conclusions

In this thesis, we have theorized a Software Defined Radio platform capable of decoding information from two heterogeneous wireless standards simultaneously using a single RF front-end. We termed it Simultaneous Multi-Standard SDR (SMS-SDR). Our target networks are random access networks such as IEEE 802.11g, IEEE 802.11ac, IEEE 802.11ax, LTE-LAA, IEEE 802.15.4 operating in unlicensed 2.4 and 5 GHz bands. In the unlicensed bands, these standards operate without any centralized coordination and face severe Cross technology Co-Channel Interference (CT-CCI) as their frequency bands of operation overlaps. Among many other challenges such as finite ADC bit width, channelization, and CT-CCI, we found CT-CCI as a significant one to be addressed to realize an SMS-SDR. Besides, CT-CCI can be addressed by programming in software without any hardware based modification. We extensively studied CT-CCI and developed various physical layer signal processing methods for CT-CCI mitigation in single and multi-antenna receivers. Our major objective was to detect the simultaneous arrival (collision) of signals and recover the signals from the collided frames. While the development, we focus on the methods which can operate at the receiver in a standalone fashion, i.e., without any cooperation from the transmitter or the base station. In this way, they are suitable for random access networks operating in the license-free bands. Besides, the algorithms can be integrated into the existing infrastructure without any significant effort. We paid special attention to wireless standards which use OFDM for their physical layer because OFDM is one of the dominant PHY in the contemporary and upcoming wireless standards. Nonetheless, we chose other standards too with heterogeneous PHY to develop generic CT-CCI mitigation methods. Finally, we developed two different types of decision trees. First to detect the simultaneous arrival of two heterogeneous signals. Once the simultaneous arrival is confirmed, the next type of decision trees provides a step-by-step approach to mitigate the interference based on the characteristics of the signals. Nonetheless, the applicability of the decision trees are not restricted by the characteristics of the signals and can be used for any two heterogeneous/homogeneous signals. In the next phase of our work, we implemented

our selective CT-CCI mitigation algorithms using General Purpose Processor based SDR. We used GNU Radio and Openairinterface as the SDR software package and USRP as the SDR hardware. We performed over-the-air tests using standard compliant waveforms and found the results to be in close agreement with the simulation results. The tests also validates the applicability of our algorithms for real-life practical scenarios.

8.2 Future Work

To realize an SMS-SDR, mitigation of CT-CCI is one of the steps which is addressed in this thesis. Nonetheless, there are significant hurdles to be solved before a full-fledged SMS-SDR can be realized. Finite ADC bit width is a fundamental problem among them. It could become a decisive factor if the power level of one signal is very high compared to the other. In such cases, even sophisticated algorithms such as Successive Interference Cancellation may fail to recover the weaker signal. As discussed in Chapter 2, solutions have been proposed which require modification in the hardware architecture and have the potential to receive signals of different power levels using single RF front-end.

Another potential continuation to our work could be the development of SMS-SDR which is also capable of "transmitting" multiple heterogeneous wireless signals simultaneously. We foresee two challenges in simultaneous transmission. Unlike the ADC, the finite bitwidth of DAC is not problematic here and can be trivially solved. However, a more significant challenge will be interference between the two signals as soon as they are transmitted from the transmitter itself. This will be in contrast to the case of the receiver where signals come from different sources. Methods such as self-interference cancellation being researched in the context of full-duplex communication [44][106] can be used to solve the problem of simultaneous transmissions in a multi-antenna SMS-SDR transmitter.

Nonetheless, our works have significant potential for application and expansion in the upcoming 5G networks, where problems arising due to interference have been foreseen. Two such areas are as follows:

- Co-existence between 5G services such as eMBB, URLLC and, mMTC [67] where interference management is foreseen as one of the challenging tasks. Among many proposed solutions, NOMA[26] based methods (which also includes SIC) are being developed for efficient utilization of resources.

- Interference management in Ultra-Dense Network (UDN) where the dense and random deployment of heterogeneous network infrastructures results in unpredictable interference patterns compared to sparse networks [64].

Appendix A

A.1 Round Trip and Receive Latency Measurement in USRP

This measurement is conducted in order to estimate the round trip and receive latency for USRP B210 and USRP X300. The measured latency is used to investigate GPP based bidirectional 802.11g SDR implementation feasibility.

Critical SIFS requirement for bidirectional 802.11g transceiver

- SIFS is the time from the reception of the last PPDU symbol to the transmission of the first symbol of the response PPDU.
- SIFS for 802.11a (5GHz band) is 16 microsecs and 802.11g (2.4 GHz) is 10 microsecs.
- Additionally in order to transmit any type of frame in the air, 802.11 follows CSMA/CA with DCF among the transmitting stations. Once the channel is sensed idle, the transmitter has to respond instantaneously. Delay in response may result in false channel information and hence collision of packets in air.

Test Methods

We conduct two different tests. One for measuring the round trip latency and another for receive latency for both the aforementioned USRPs. We use UHD (Universal Hardware Driver) API in order to stream samples from USRP to CPU and vice versa. Following hardware were used in the tests :

- LeCroy 6050 : 500 MHz Oscilloscope
- Rohde&Schwarz VSG SMB 100
- USRP B210
- USRP X300
- Dell Precision 5510 (For USRP B210)

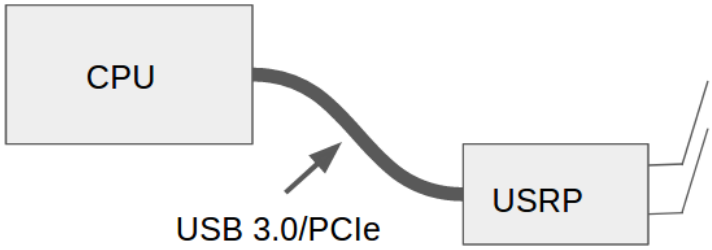


Fig. A.1. Round trip latency test setup for USRP B210 and USRP X300

- Intel(R) Xeon(R) CPU E5-2687W v3 @ 3.10GHz (For USRP X300)

Sampling rate of 20 MHz with a center frequency of 400 MHz was used.

Round Trip Latency Test method

For round trip latency test, we use the script latency_test.cpp which is provided by UHD. It can be found in /uhd/host/examples. This script receives a packet at time t and tries to send the same packet at time t + rtt, where rtt is the requested round trip time(round trip time sample time from device to host and back to the device). rtt can be inputted to the script as command line parameter. The script takes rtt as input and tries to perform the mentioned routine and outputs if there were underruns or overruns in form of ACK. For a success, the number of ACK received has to equal to number of runs. The test was conducted with 100 samples per run and 1000 runs in total. We changed the default values of following parameters in order to minimize the latency as much as possible. We tuned the parameters till there were no overflows and underflows. Finally following values were used. Params mentioned in bold in Table 1 are valid only for USB based transfer(USRP B210) and not for

USRP B210	**USRP X300**
(”sc16”, ”sc16”)	(”sc16”, ”sc16”)
”spp” = ”80”	”spp” = ”80”
”num_recv_frames” = ”256”	
”recv_frame_size” = ”20”	
”num_send_frames” = ”256”	
”send_frame_size” = ”20”	

Table A.1: UHD stream args used for latency_test.cpp

PCIe(USRP X300) based transfer between USRP and CPU. The test setup is shown in Fig. A.1

Observations

Minimum rtt supported by USRP B210 was 160 micro secs while 75 micro secs for USRP X300 for the configurations mentioned in Table 1.

Receive Latency Test Method

For receiver latency test, we made a custom script in C++ using UHD C++ API. A signal generator(VSG) was taken and configured to continuously transmit 802.11g frames at an inter-frame interval of 100ms. The 802.11g signal was splitted and fed to oscilloscope and USRP simultaneously. USRP was set into receiver mode at a sampling rate of 20 MHz. The sampled data from USRP was fed to CPU. The script continuously compares the average energy over a window of samples and compares it against a threshold. Size of window was equal to size of the buffer(mentioned below as spp). If window energy exceeds the threshold, the script triggers all the GPIO pins on the USRP to go HIGH, which were otherwise LOW. The GPIO pins of the USRP were connected to the other channel of oscilloscope and the delay between the transmit signal from signal generator was being continuously compared. We used following parameters to configure the USRPs thru UHD. Measured time highly depends on transport parameters (for USRP B210) and samples per packet parameter (spp for both USRPs). Similar to round trip latency test, we tried to put spp parameter as less as possible till there were no overruns. However receive latency tests (for both USRP B210 and X300), did not comply with spp value of 80 which was used in round trip latency tests. One of the possible reasons could be continuous streaming of samples in receiver latency tests vs non-continuous streaming of samples in round trip latency test. A large size of spp will leads to higher latency as the USRP buffer wait for the buffer to be filled up before flushing it to the CPU. Parameters mentioned in bold in Table

USRP B210	**USRP X300**
stream_args("sc16", "sc16")	stream_args("sc16", "sc16")
stream_args.args["spp"] = "500"	stream_args.args["spp"] = "200"
stream_args.args["num_recv_frames"] = "256"	
stream_args.args["recv_frame_size"] = "20"	
stream_args.args["num_send_frames"] = "256"	
stream_args.args["send_frame_size"] = "20"	

Table A.2: UHD Params used for Receive Latency Test

2 are valid only for USB based transfer(USRP B210) and not for PCIe(USRP X300) based transfer between USRP and CPU. The test setup and hardware are shown in Figure 2 and 3 respectively Figure 4 shows the latency measurement from LeCroy Oscilloscope In Figure 4 the blue line is from signal generator while the yellow line is from GPIO. Delay is continuously been tracked (arrow mark). Figure 5 shows the calculation of receive latency as "Measured Time"

Observations

The measured time was highly fluctuating, hence we took statistical measurements by obtaining the histogram of the delay. Results from the histogram are shown in Table 3

Histogram of the receive latency for B210 and X300 are shown in Figure 6 and 7 respectively.

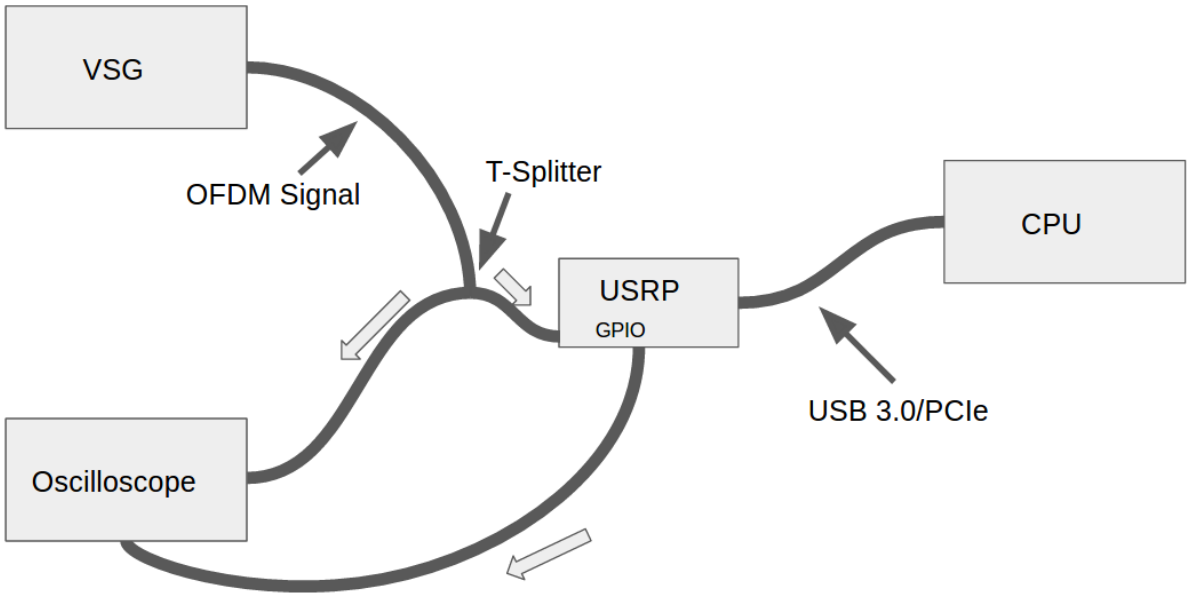


Fig. A.2. Receive latency test setup for USRP B210 and USRP X300

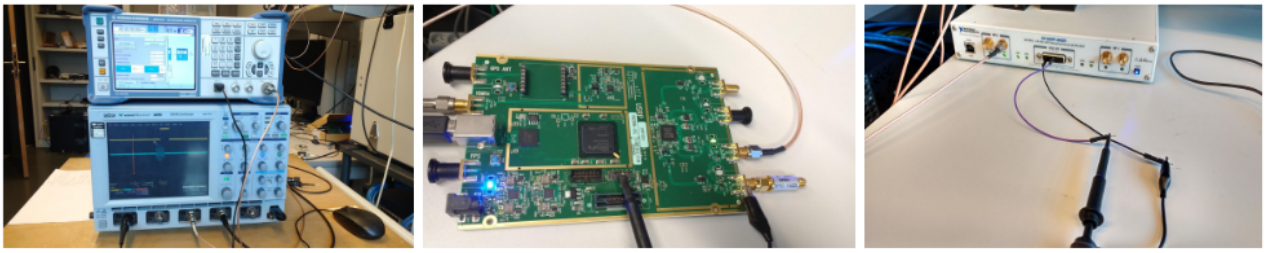


Fig. A.3. Hardware Setup

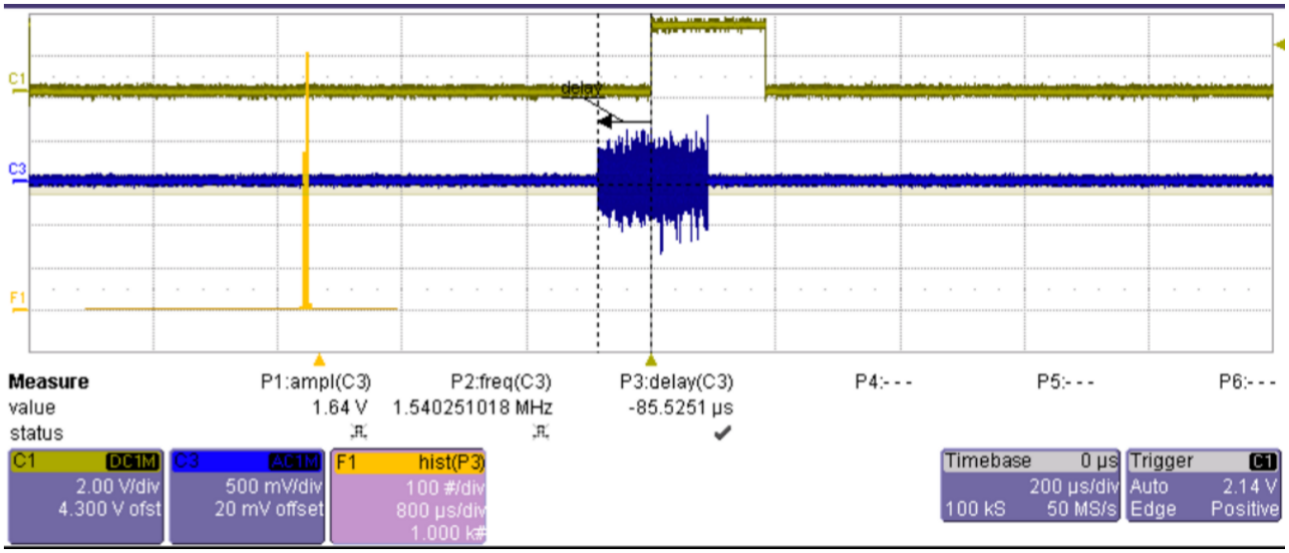


Fig. A.4. Manual view of receive latency on Oscilloscope

	USRP B210	**USRP X300**
Maxm Latency (μs)	126	105
Minm Latency (μs)	68.8	57.6
Mode (μs)	88.8	83.6

Table A.3: Receive latency test results

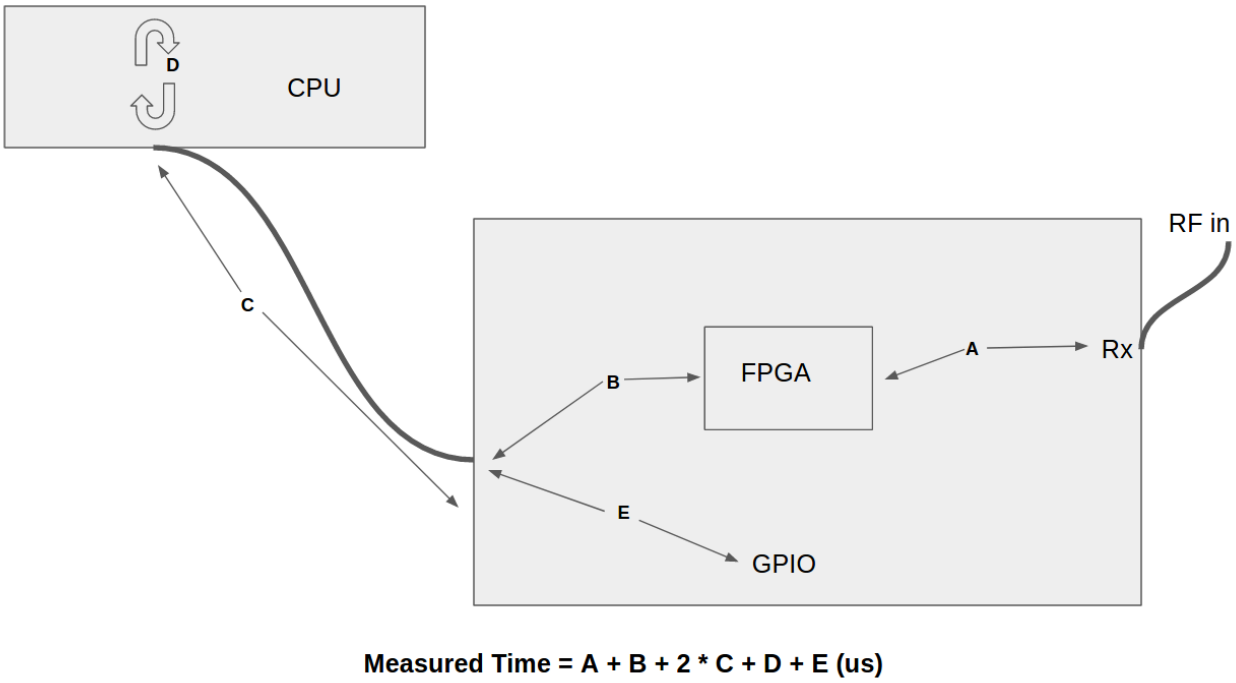


Fig. A.5. Components contributing to receive latency

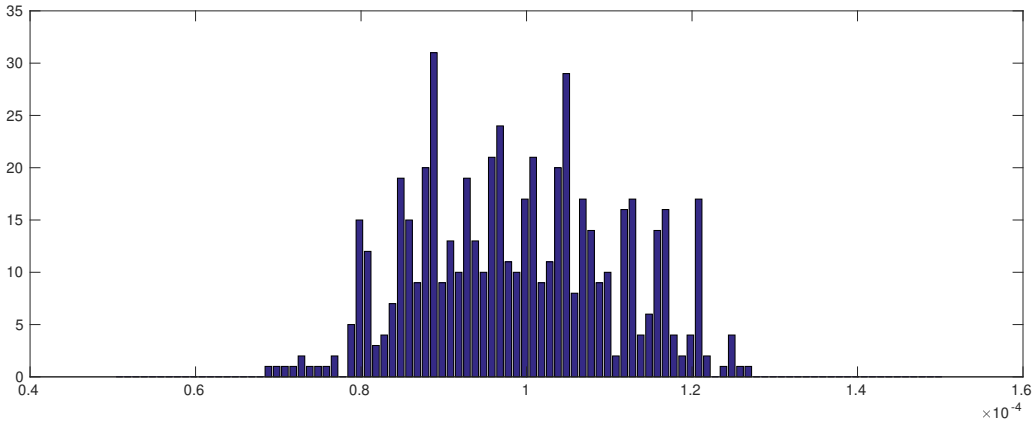


Fig. A.6. Receive Latency for B210

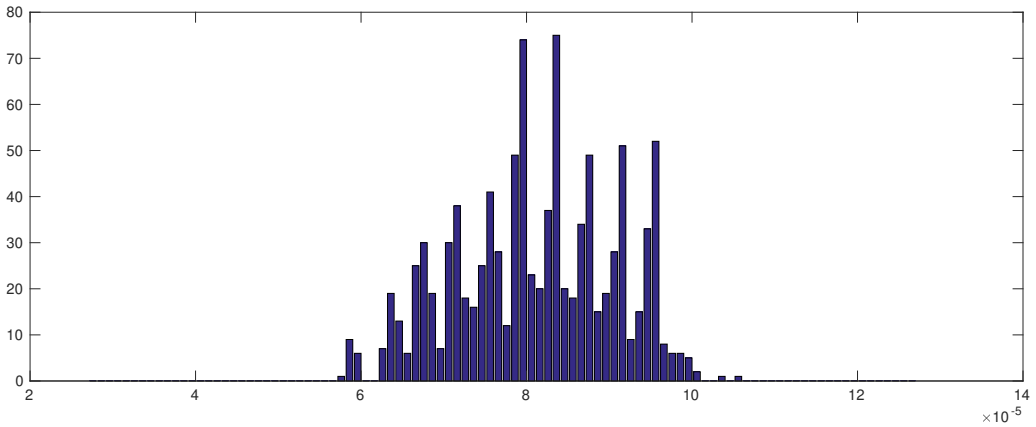


Fig. A.7. Receive Latency for X300

Conclusion

Half of the measured time gives a rough indication of latency. We observe that with the current GPU based architecture to implement bidirectional WiFi (802.11g – SIFS 10 microsecs) is not feasible with such delays using USRP X300 (PCIe) and USRP B210 (USB 3.0).

Appendix B

B.1 Soft Bit Metrics

A hard decision receiver loses the reliability of decision since the decision is binary, i.e., 0 or 1. A soft decision receiver takes into account the reliability symbols before making any decision. In order to compute the reliability of symbols, a soft decision receiver computes the soft bit metrics. In an OFDM system, soft bit metrics can be written as:

$$\gamma(i,l,p) = \min_{z \in Z_p^l} ||Y - Hz||^2 \tag{B.1}$$

where Y is the received sample, h is the channel estimate, z is the symbol constellation and $\gamma(i,l,p)$ is the soft bit metrics for the l-th bit and i-th subcarrier to be p, where p is either 0 or 1. Z_p^l is the subset of constellation points such that the i-th bit is equal to p. The physical interpretation of (B.1) is computing the minimum distance between the received symbol and projection of constellation points for a given bit. Let's take the example of QPSK, where a symbol consists of 2 bits (say 0-th bit b0 and 1st bit b1). Thus any QPSK symbol is made by the concatenation b0b1 where b0 and b1 can take the value of 0 or 1. This is shown in Fig. B.1. The soft bit metrics corresponding to i-th subcarrier of OFDM are computed as follows:

$\gamma(i,0,0)$ = soft bit metrics for 0-th bit to be 0 = $\min(d_{00}, d_{01})$

$\gamma(i,0,1)$ = soft bit metrics for 0-th bit to be 1 = $\min(d_{10}, d_{11})$

$\gamma(i,1,0)$ = soft bit metrics for 1-st bit to be 0 = $\min(d_{00}, d_{10})$

$\gamma(i,1,1)$ = soft bit metrics for 1-st bit to be 1 = $\min(d_{01}, d_{11})$

where d_{mn} represents the Euclidean distance between the received symbol and the constellation point (m,n). The soft bit metrics pair ($\gamma(i,0,0)$,$\gamma(i,0,1)$) and ($\gamma(i,1,0)$,$\gamma(i,1,1)$) are sent to Viterbi decoder for further processing. For higher modulation schemes, the soft bit metrics calculation is intuitive. For example, in a 16QAM system, there will 4 bits and 64QAM system, there will be 6 bits in a symbol.

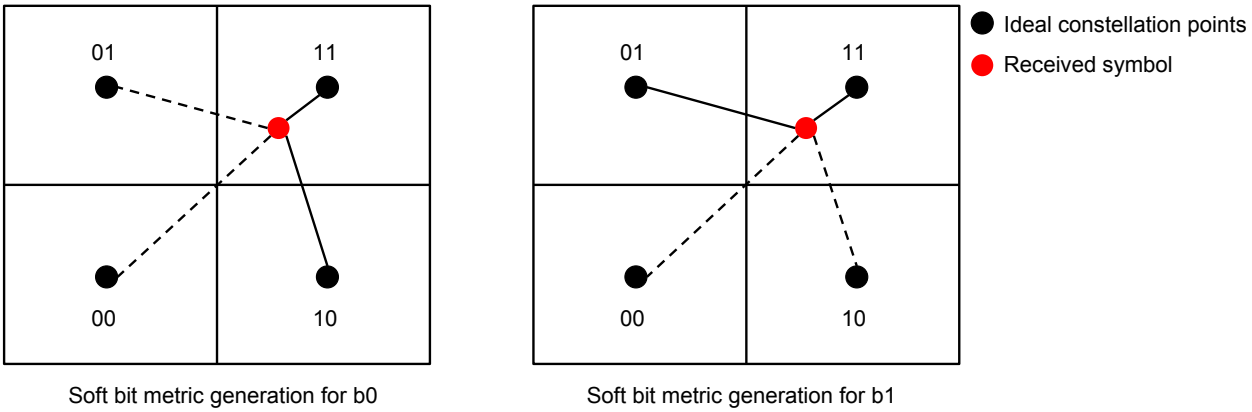


Fig. B.1. Soft bit metrics calculation in QPSK

B.2 Soft Bit Maximal Ratio Combiner (SBMRC)

Soft Bit Maximal Ratio Combiner is a different yet equally efficient method to implement diversity Combining in multi-antenna systems. SBMRC is more popular in distributed systems [74][81]. In contrast to the conventional diversity combining scheme such as MRC which combines complex samples obtained from the different antenna branches, an SBMRC combines the soft bit metrics from individual antenna branches. Now we develop expression for bit metrics computation in a multi-antenna system following soft bit maximal ratio combining. We consider a dual antenna OFDM receiver. According to SBMRC [74, Eq-11] soft bit metrics corresponding to the i-th subcarrier and l-th bit computed from the samples obtained from the two antennas can be written as:

$$\gamma(i,l,p)_{\text{SBMRC}} = \min_{z \in Z_p^l} ||\mathbf{Y} - \mathbf{H}z||^2 \tag{B.2}$$

Where $\mathbf{Y} = \begin{pmatrix} Y_1(i) \\ Y_2(i) \end{pmatrix}$ is the vector of received samples; $\mathbf{H} = \begin{pmatrix} H_{z_1}(i) \\ H_{z_2}(i) \end{pmatrix}$ is the vector of channel estimates; and $\gamma(i,l)_{\text{SBMRC}}$ is the combined soft bit metrics after SBMRC. The expression for $\gamma(i,l)_{\text{SBMRC}}$ can be further expanded as follows:

$$= \min_{z \in Z_0^l} \left\| \begin{pmatrix} Y_1(i) \\ Y_2(i) \end{pmatrix} - \begin{pmatrix} H_{z_1}(i) \\ H_{z_2}(i) \end{pmatrix} z \right\|^2 \tag{B.3}$$

$$\approx \min_{z \in Z_p^l} (||Y_1(i) - H_{z_1}(i)z||^2) + \min_{z \in Z_p^l} (||Y_2(i) - H_{z_2}(i)z||^2)$$

$$= \min_{z \in Z_p^l} (||Y_1(i) - H_{z_1}(i)z||^2) + \min_{z \in Z_p^l} (||Y_2(i) - H_{z_2}(i)z||^2)$$

$$= \gamma(i,l)_1 + \gamma(i,l)_2 \tag{B.4}$$

Expression (B.4) is nothing but addition of soft bit metrics of l-th bit corresponding to i-th subcarrier $\gamma(i,l)_1$ and $\gamma(i,l)_2$ from the two antenna branches respectively. In the next step, these soft bit metrics are sent to the FEC decoder for further processing.

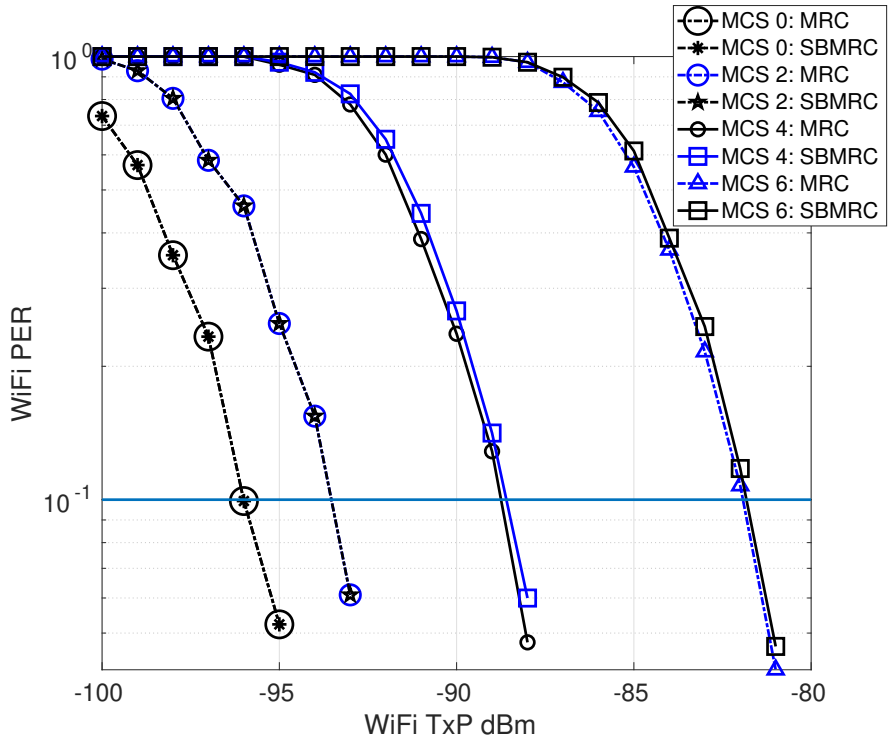


Fig. B.2. MRC vs SBMRC in the absence of interference. Both of them perform the same in the absence of interference under the same channel conditions.

Discussing further, soft bit metrics is a quantification of the characteristic of the bit; usually reflective of the bit SNR or reliability. A similar metrics can be obtained by computing the Log Likelihood Ratios (LLRs) of the bits, and the LLRs are sent to the FEC decoder. Whether to send soft bit metrics or the LLRs to the FEC decoder depends on the implementation of the FEC decoder. For example, the FEC decoder implementation for IEEE 802.11g and LTE in MATLAB 2018a expects LLRs as input while the FEC decoder implementation for IEEE 802.15.4 in MATLAB 2018a expects soft bit metrics. Nonetheless, in order to perform diversity combining, the LLRs can be combined, i.e., as the soft bit metrics have been added as in (B.4).

Achieving diversity combining by adding the soft bit metrics or LLRs simplifies the way it can be implemented in SDR software. Especially, for our case, a diversity combiner module was not readily available in GNU Radio; however, obtaining LLRs corresponding to IEEE 802.11g bit was simple. Hence, we chose SBMRC as our diversity combining scheme for the SDR implementation. We perform simulations to compare the performance of SBMRC and MRC for a dual antenna IEEE 802.11g receiver under the same channel conditions and in the absence of interference. As a performance metric, we choose IEEE 802.11g Transmit power required to obtain a Packet Error Rate (PER) of 10% [46] for MRC and SBMRC. Correlation between channels of the two antenna is fixed to 0.4 based on the measurements listed in [49]. Results are plotted in Fig. B.2. For the 10% PER criterion, we observe that both MRC and SBMRC essentially perform the same for IEEE 802.11g MCS 0 and 2 while SBMRC shows a slight gain at higher IEEE 802.11g MCS, i.e., 4 and 6. This equivalence in

performance between MRC and SBMRC encourages our choice of using SBMRC instead of MRC for achieving diversity gain as the implementation of SBMRC is simpler using SDR software packages. On the downside, the complexity of SBMRC may increase with the increase of the constellation size; because each branch of the receiver is now involved in the computation of LLRs. Nonetheless, actual LLRs can be approximated by approx LLRs to ease the computation. In Chapter 4 and Chapter 5, we have used SBMRC to implement MLSC, DC-TIMO, and SIC-MRC by combining the approx LLRs corresponding to different antenna branches.

B.3 Computation of Log Likelihood Ratio

Log Likelihood Ratio is a way to compute the soft bit metrics. Depending on the implementation of the FEC decoder, either LLRs or soft bit metrics are fed as input to the FEC decoder. LLR computation for a BPSK system can be performed as follows:

$$L(z|Y) = \ln \frac{P[z=+1|Y]}{P[z=-1|Y]} \tag{B.5}$$

where $L(z|Y)$ is the a posteriori L-value. Using Bayes's rule it can be shown that

$$\underbrace{L(z|Y)}_{\text{a posteriori L-value}} = \ln \frac{p(Y|z=+1)P[z=+1]}{p(Y|z=-1)P[z=-1]} = \underbrace{\ln \frac{P[z=+1]}{P[z=-1]}}_{\text{a priori L-value } L_A(z)} + \underbrace{\ln \frac{p(Y|z=+1)}{p(Y|z=-1)}}_{\text{channel L-value } L_{ch}(z|Y)} = L_A(z)+L_{ch}(z|Y). \tag{B.6}$$

In (B.6), the channel L-value is an indicator of the information obtained about the transmitted symbol z based on the observation of received symbol Y. $L_{ch}(z|Y)$ for an AWGN channel with zero mean and variance σ^2 can be computed as:

$$L_{ch}(z|Y) = \ln \frac{\exp(-\frac{(Y-1)^2}{2\sigma^2})}{\exp(-\frac{(Y+1)^2}{2\sigma^2})} = \frac{2}{\sigma^2}Y. \tag{B.7}$$

$L_{ch}(z|Y)$ is also termed as LLR. If the transmitted symbol is constructed using M bits per symbol, then M individual L-values per symbol are required to be computed as we did while computing the soft bit metrics for QPSK symbols in the previous section. The channel L-value in this case can be written as follows:

$$L_{ch}(g_l|Y) = \ln \frac{\sum_{\mathbf{g}\in\mathbb{G}_{l,1}} p(Y|\mathbf{z}) \cdot \exp\left[\sum_{g_k=1,k\neq l} L_A(g_k)\right]}{\sum_{\mathbf{g}\in\mathbb{G}_{l,0}} p(Y|\mathbf{z}) \cdot \exp\left[\sum_{g_k=1,k\neq l} L_A(g_k)\right]} \tag{B.8}$$

Where $\mathbb{G}_{l,p}$ is the set of symbols $\mathbf{z}$ for which $g_l = p$, and p can take the value 0 or 1. This the LLR of l-th bit can be written as:

$$L(g_l|Y) = \underbrace{\ln \frac{P[g_l = 1]}{P[g_l = 0]}}_{L_A(g_l)} + L_{ch}(g_l|Y) \tag{B.9}$$

Bibliography

[1] 5G UE Demonstrator using Openairinterface. www.openairinterface.org. Accessed: 2018-11-16.

[2] Broadcom BCM43012. https://www.broadcom.com/products/wireless/wireless-lan-bluetooth/bcm43012. Accessed: 2018-11-16.

[3] Cypress CYW43012. http://www.cypress.com/products/wi-fi-bluetooth-combos. Accessed: 2018-11-16.

[4] Daughter Boards, Ettus Research. https://www.ettus.com/product/category/Daughterboards. Accessed: 2018-11-16.

[5] Design and Prototype SDR systems with Matlab and Simulink. https://www.mathworks.com/discovery/sdr.html. Accessed: 2018-11-16.

[6] GNU Radio. https://gnuradio.org. Accessed: 2018-11-16.

[7] Labview Communications 802.11 Application Framework 1.1 White Paper. http://www.ni.com/product-documentation/52533/en/. Accessed: 2018-11-16.

[8] Microsoft Research Software Radio (sora). https://www.microsoft.com/en-us/research/project/microsoft-research-software-radio-sora/. Accessed: 2018-11-16.

[9] Software Radio (SDR). http://www.ni.com/fr-fr/innovations/wireless/software-defined-radio.html. Accessed: 2018-11-16.

[10] Universal Software Radio Peripheral (usrp). https://www.ettus.com. Accessed: 2018-11-16.

[11] WARP: Wireless Open Access Research Platform. https://warpproject.org/trac. Accessed: 2018-11-16.

[12] Tarjei Aaberge. Low complexity antenna diversity for IEEE 802.15. 4 2.4 GHz PHY. Master's thesis, Institutt for elektronikk og telekommunikasjon, Norwegian University of Science and Technology, 2009.

[13] Vignesh Adhinarayanan, Thaddeus Koehn, Krzysztof Kepa, Wu-chun Feng, and Peter Athanas. On the performance and energy efficiency of FPGAs and GPUs for polyphase channelization. pages 1–7, 2014.

[14] Rana Ahmed, Ben Eitel, and Joachim Speidel. Enhanced maximum ratio combining for mobile DVB-T reception in doubly selective channels. In *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, pages 1–5. IEEE, 2015.

[15] Minsik Ahn, Dongsu Kim, and J Stevenson Kenney. Throughput improvement in interference limited multipath environments using a smart antenna for ieee 802.11 b wlan. In *Radio and Wireless Conference, 2004 IEEE*, pages 411–414. IEEE, 2004.

[16] Islam Alyafawi, Arnaud Durand, and Torsten Braun. High-performance wideband sdr channelizers. In *International Conference on Wired/Wireless Internet Communication*, pages 3–14. Springer, 2016.

[17] Jeffrey G Andrews. Interference cancellation for cellular systems: a contemporary overview. *IEEE Wireless Communications*, 12(2):19–29, 2005.

[18] Vangelis Angelakis, Nikos Kossifidis, Stefanos Papadakis, Vasilios Siris, and Apostolos Traganitis. The effect of using directional antennas on adjacent channel interference in 802.11 a: Modeling and experience with an outdoors testbed. In *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, 2008. WiOPT 2008. 6th International Symposium on*, pages 24–29. 2008.

[19] Babak Azimi-Sadjadi, Daniel Sexton, Ping Liu, and Michael Mahony. Interference effect on IEEE 802.15.4 performance. In *Proceedings of 3rd international conference on networked sensing systems (INNS), Chicago, IL*. 2006.

[20] Alireza Babaei, Jennifer Andreoli-Fang, Yimin Pang, and Belal Hamzeh. On the impact of LTE-U on Wi-Fi performance. *International Journal of Wireless Information Networks*, 22(4):336–344, 2015.

[21] Fulvio Babich and Massimiliano Comisso. Throughput and delay analysis of 802.11-based wireless networks using smart and directional antennas. *IEEE Transactions on Communications*, 57(5), 2009.

[22] SA Bassam, MM Ebrahimi, A Kwan, M Helaoui, MP Aflaki, O Hammi, M Fattouche, and FM Ghannouchi. A generic architecture for smart multi-standard software defined radio systems. In *SDR'09 Technical Conference and Product Exposition*, pages 1–4, 2009.

[23] Boris Bellalta. IEEE 802.11ax:high-efficiency WLANs. *IEEE Wireless Communications*, 23(1):38–46, 2016.

[24] B Bloessl. IEEE 802.15.4 Transceiver. https://github.com/bastibl/gr-ieee802-15-4, 2018. Accessed: 2018-11-16.

[25] Bastian Bloessl. IEEE 802.11 a/g/p Transceiver. https://github.com/bastibl/gr-ieee802-11, 2018. Accessed: 2018-11-16.

[26] Ishan Budhiraja, S Tyagi, Sudeep Tanwar, Neeraj Kumar, and Joel Jose Rodrigues. Tactile internet for smart communities in 5g: An insight for noma-based solutions. *IEEE Transactions on Industrial Informatics*, 2019.

[27] Viveck R Cadambe, Syed A Jafar, and Shlomo Shamai. Interference alignment on the deterministic channel and application to fully connected gaussian interference networks. *IEEE Transactions on Information Theory*, 55(1):269–274, 2009.

[28] Mario Cagalj, Saurabh Ganeriwal, Imad Aad, and J-P Hubaux. On selfish behavior in csma/ca networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 4, pages 2513–2524. 2005.

[29] Cristina Cano, David López-Pérez, Holger Claussen, and Douglas J Leith. Using lte in unlicensed bands: Potential benefits and coexistence issues. *IEEE communications magazine*, 54(12):116–123, 2016.

[30] Christopher J Corbett, Warren V Barkley, and Amer Aref Hassan. Using directional antennas to mitigate the effects of interference in wireless networks. October 31 2006. US Patent 7,130,586.

[31] Pedro Miguel Cruz and Nuno Borges Carvalho. Enhanced architecture to increase the dynamic range of sdr receivers. In *Radio and Wireless Symposium (RWS), 2011 IEEE*, pages 331–334. 2011.

[32] Jian Cui, David D Falconer, and Asrar UH Sheikh. Performance evaluation of optimum combining and maximal ratio combining in the presence of co-channel interference and channel correlation for wireless communication systems. *Mobile Networks and Applications*, 2(4):315–324, 1997.

[33] Andrea Goldsmith. *Wireless communications*. Cambridge university press, 2005.

[34] Shyamnath Gollakota, Fadel Adib, Dina Katabi, and Srinivasan Seshan. Clearing the RF smog: making 802.11n robust to cross-technology interference. In *ACM SIGCOMM Computer Communication Review*, volume 41, pages 170–181. ACM, 2011.

[35] Shyamnath Gollakota, Samuel David Perli, and Dina Katabi. Interference alignment and cancellation. In *ACM SIGCOMM Computer Communication Review*, volume 39, pages 159–170. 2009.

[36] Shyamnath Shyamnath Venkata Satyasrisai Gollakota. *Embracing interference in wireless systems.* PhD thesis, Massachusetts Institute of Technology, 2012.

[37] Michelle X Gong, Brian Hart, and Shiwen Mao. Advanced wireless LAN technologies: IEEE 802.11ac and beyond. *GetMobile: mobile computing and communications*, 18(4):48–52, 2015.

[38] Albert Gran, Shih-Chun Lin, and Ian F Akyildiz. Towards wireless infrastructure-as-a-service (WlaaS) for 5g software-defined cellular systems. In *Communications (ICC), 2017 IEEE International Conference on*, pages 1–6. IEEE, 2017.

[39] Daniel Halperin, Thomas Anderson, and David Wetherall. Taking the sting out of carrier sense: interference cancellation for wireless lans. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 339–350. 2008.

[40] Mengqi Han, Sami Khairy, Zhao Chen, Lin X Cai, and Yu Cheng. A performance comparison of lbe based coexistence protocols for laa and wi-fi. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.

[41] H Harada, R Funada, Y Shoji, R Kimura, Y Nishiguchi, M Lei, and C Choi. IEEE P802.15 working group for wireless personal area networks (WPANs). *IEEE P802*, 15, 2007.

[42] Harri Holma and Antti Toskala. *WCDMA for UMTS: HSPA evolution and LTE.* John Wiley & sons, 2007.

[43] Harri Holma and Antti Toskala. *LTE for UMTS: OFDMA and SC-FDMA based radio access.* John Wiley & Sons, 2009.

[44] S. Hong, J. Brand, J. I. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis. Applications of self-interference cancellation in 5g and beyond. *IEEE Communications Magazine*, 52(2):114–121, February 2014.

[45] Yantian Hou, Ming Li, Xu Yuan, Y Thomas Hou, and Wenjing Lou. Cooperative cross-technology interference mitigation for heterogeneous multi-hop networks. In *INFOCOM, 2014 Proceedings IEEE*, pages 880–888. 2014.

[46] IEEE Computer Society LAN MAN Standards Committee and others. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *ANSI/IEEE Std. 802.11-1999*, 1999.

[47] Aleksandar Jeremic, Timothy A Thomas, and Arye Nehorai. Ofdm channel estimation in the presence of interference. *IEEE transactions on signal processing*, 52(12):3429–3439, 2004.

[48] Yubing Jian, Chao-Fang Shih, Bhuvana Krishnaswamy, and Raghupathy Sivakumar. Coexistence of Wi-Fi and LAA-LTE: Experimental evaluation, analysis and insights. In *Communication Workshop (ICCW), 2015 IEEE International Conference on*, pages 2325–2331. 2015.

[49] Padam L Kafle, Apichart Intarapanich, Abu B Sesay, John McRory, and Robert J Davies. Spatial correlation and capacity measurements for wideband mimo channels in indoor office environment. *IEEE Transactions on wireless communications*, 7(5), 2008.

[50] Florian Kaltenberger, Xiwen Jiang, and Raymond Knopp. From massive MIMO to C-RAN: the OpenAirInterface 5G testbed. In *ASILOMAR 2017, Asilomar Conference on Signals, Systems, and Computers, October 29th-November 1st 2017, Pacific Grove, CA, USA*, Pacific Grove, ÉTATS-UNIS, 10 2017.

[51] Florian Kaltenberger, Raymond Knopp, Navid Nikaein, Dominique Nussbaum, Lionel Gauthier, and Christian Bonnet. Openairinterface: Open-source software radio solution for 5g. In *European Conference on Networks and Communications (EUCNC), Paris, France*, 2015.

[52] Jerzy Konorski. A game-theoretic study of csma/ca under a backoff attack. *IEEE/ACM Transactions on Networking (TON)*, 14(6):1167–1178, 2006.

[53] Sumit Kumar. Soft decision viterbi decoder for wifi. `https://github.com/sumitstop/SDVD-WiFi`, Nov 2018.

[54] Sumit Kumar, Florian Kaltenberger, Alejandro Ramirez, and Bernhard Kloiber. A robust decoding method for ofdm systems under multiple co-channel narrowband interferers. In *2018 European Conference on Networks and Communications (EuCNC)*, pages 368–372. IEEE, 2018.

[55] Sumit Kumar, Florian Kaltenberger, Alejandro Ramirez, and Bernhard Kloiber. Robust OFDM diversity receiver under co-channel narrowband interference. In *WIMOB 2018, 14th International Conference on Wireless and Mobile Computing, Networking and Communications, 15-17 October 2018, Limassol, Cyprus*, Limassol, CHYPRE, 10 2018.

[56] Sumit Kumar, Florian Kaltenberger, Alejandro Ramirez, and Bernhard Kloiber. A WiFi SIC receiver in the presence of LTE-LAA for indoor deployment. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018.

[57] Swarun Kumar, Diego Cifuentes, Shyamnath Gollakota, and Dina Katabi. Bringing cross-layer mimo to today's wireless lans. In *ACM SIGCOMM Computer Communication Review*, volume 43, pages 387–398. 2013.

[58] Yang Lan, Lihui Wang, Huiling Jiang, Kazuki Takeda, Hiroki Harada, Satoshi Nagata, Tang Wenfang, and Li Qiang. A field trial of lte in unlicensed bands with sdl (supplemental downlink) transmission. In *Wireless Communications and Networking Conference (WCNC), 2016 IEEE*, pages 1–5. IEEE, 2016.

[59] Jingu Lee, Minho Kim, Daehyun Kim, Jonghwa Lee, Jungyeol Kim, and Younglok Kim. Methods of channel estimation and symbol detection for ieee 802.15. 4 considering the wireless channel in the high speed train. *Journal of Advances in Computer Networks*, 3(3), 2015.

[60] Weon-Cheol Lee, Choul-Hee Cho, Jong-Ho Kwak, Min-Young Park, and Kyung-Jin Kang. Viterbi decoding method using channel state information in COFDM system. In *Consumer Electronics, 1999. ICCE. International Conference on*, pages 66–67. IEEE, 1999.

[61] Li Erran Li, Z Morley Mao, and Jennifer Rexford. Toward software-defined cellular networks. In *Software Defined Networking (EWSDN), 2012 European Workshop on*, pages 7–12. IEEE, 2012.

[62] Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, and Andreas Terzis. Surviving WiFi interference in low power ZigBee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, pages 309–322. ACM, 2010.

[63] Kate Ching-Ju Lin, Shyamnath Gollakota, and Dina Katabi. Random access heterogeneous mimo networks. In *ACM SIGCOMM Computer Communication Review*, volume 41, pages 146–157. 2011.

[64] Junyu Liu, Min Sheng, Lei Liu, and Jiandong Li. Interference management in ultra-dense networks: Challenges and approaches. *IEEE Network*, 31(6):70–77, 2017.

[65] Zhigang Luo, Wei Li, Yan Zhang, and Wei Guan. Method for multi-standard software defined radio base-band processing, August 24 2010. US Patent 7,784,028.

[66] Ingo Lütkebohle. NVIDIA i500 whitepaper FINALv3. `https://www.nvidia.com/docs/IO/116757/NVIDIA_i500_whitepaper_FINALv3.pdf`, 2014. [Online; accessed 21-Jan-2019].

[67] Andrea Matera, Rahif Kassab, Osvaldo Simeone, and Umberto Spagnolini. Non-orthogonal embb-urllc radio access for cloud radio access networks with analog fronthauling. *Entropy*, 20(9):661, 2018.

[68] Baher Mawlawi and Jean-Baptiste Doré. Csma/ca with rts/cts overhead reduction for m2m communication with finite retransmission strategy. In *IEEE International Wireless Communications & Mobile Computing Conference*, 2015.

[69] Christian Mehlführer, Martin Wrulich, Josep Colom Ikuno, Dagmar Bosanska, and Markus Rupp. Simulating the long term evolution physical layer. In *Signal Processing Conference, 2009 17th European*, pages 1471–1478. IEEE, 2009.

[70] Nikolaos I Miridakis and Dimitrios D Vergados. A survey on the successive interference cancellation performance for single-antenna and multiple-antenna ofdm systems. *IEEE Communications Surveys & Tutorials*, 15(1):312–335, 2013.

[71] Nikolaos I Miridakis and Dimitrios D Vergados. A survey on the successive interference cancellation performance for single-antenna and multiple-antenna ofdm systems. *IEEE Communications Surveys & Tutorials*, 15(1):312–335, 2013.

[72] Hyung G Myung, Junsung Lim, and David J Goodman. Single Carrier FDMA for uplink wireless transmission. *IEEE Vehicular Technology Magazine*, 1(3):30–38, 2006.

[73] Tamer Nadeem. Analysis and enhancements for ieee 802.11 networks using directional antenna with opportunistic mechanisms. *IEEE Transactions on Vehicular Technology*, 59(6):3012–3024, 2010.

[74] Xuemei Ouyang, Monisha Ghosh, and Joseph P Meehan. Optimal antenna diversity combining for ieee 802.11 a system. *IEEE Transactions on Consumer Electronics*, 48(3):738–742, 2002.

[75] Ulrich Ramacher. Software-defined radio prospects for multistandard mobile phones. *Computer*, (10):62–69, 2007.

[76] Guangliang Ren, Huining Zhang, and Yilin Chang. SNR estimation algorithm based on the preamble for OFDM systems in frequency selective channels. *IEEE Transactions on Communications*, 57(8), 2009.

[77] Virgilio Rodriguez, Christophe Moy, and Jacques Palicot. An optimal architecture for a multi-standard reconfigurable radio: Cost-minimising common operators under latency constraints. In *IST Mobile Summit'06*, 2006.

[78] Thomas W Rondeau. On the gnu radio ecosystem. *Opportunistic Spectrum Sharing and White Space Access: The Practical Reality*, pages 25–48, 2015.

[79] Ahmad Sadek, Hassan Mostafa, Amin Nassar, and Yehea Ismail. Towards the implementation of multi-band multi-standard software-defined radio using dynamic partial reconfiguration. *International Journal of Communication Systems*, 30(17):e3342, 2017.

[80] Magnus Sandell, Filippo Tosato, and Amr Ismail. Low complexity max-log llr computation for nonuniform pam constellations. *IEEE Communications Letters*, 20(5):838–841, 2016.

[81] Akram Bin Sediq and Halim Yanikomeroglu. Performance analysis of soft-bit maximal ratio combining in cooperative relay networks. *IEEE Transactions on Wireless Communications*, 8(10), 2009.

[82] Shiann-Tsong Sheu, Yun-Yen Shih, and Wei-Tsong Lee. Csma/cf protocol for ieee 802.15. 4 wpans. *IEEE Transactions on vehicular technology*, 58(3):1501–1516, 2009.

[83] Gaotao Shi and Keqiu Li. *Signal Interference in WiFi and ZigBee Networks*. Springer, 2017.

[84] ZigBee Specification. Zigbee alliance. *ZigBee Document 053474r06, Version*, 1, 2006.

[85] MR Sriharsha, Sreekanth Dama, and Kiran Kuchi. A complete cell search and synchronization in lte. *EURASIP Journal on Wireless Communications and Networking*, 2017(1):101, 2017.

[86] Dorothy Stanley. 802.11ac-2013 - IEEE standard for information technology–telecommunications and information exchange between systems: Local and metropolitan area networks–specific requirements–part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications–amendment 4: Enhancements for very high throughput for operation in bands below 6 ghz. *IEEE-SA - The IEEE Standards Association - Home*.

[87] Gordon L Stüber. *Principles of mobile communication*, volume 2. Springer, 1996.

[88] Kun Tan, He Liu, Ji Fang, Wei Wang, Jiansong Zhang, Mi Chen, and Geoffrey M Voelker. Sam: enabling practical spatial multiple access in wireless lan. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, pages 49–60. ACM, 2009.

[89] Kun Tan, He Liu, Jiansong Zhang, Yongguang Zhang, Ji Fang, and Geoffrey M Voelker. Sora: high-performance software radio using general-purpose multi-core processors. *Communications of the ACM*, 54(1):99–107, 2011.

[90] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[91] Yu-Chee Tseng, Sze-Yao Ni, and En-Yu Shih. Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network. *IEEE transactions on computers*, 52(5):545–557, 2003.

[92] Walter HW Tuttlebee. *Software defined radio: baseband technologies for 3G handsets and basestations*. John Wiley & Sons, 2006.

[93] Gerald Ulbricht, Jakob Kneißl, Christian Kelm, and Gerd Kilian. Increasing sdr receiver dynamic range by adc diversity. *Journal of Signal Processing Systems*, 89(1):191–208, 2017.

[94] Richard Van Nee. Delay spread requirements for wireless networks in the 2.4 ghz and 5 ghz bands. *doc: IEEE P*, 802:11–97, 1997.

[95] Lochan Verma, Mohammad Fakharzadeh, and Sunghyun Choi. Wifi on steroids: 802.11 ac and 802.11 ad. *IEEE Wireless Communications*, 20(6):30–35, 2013.

[96] Andrew J. Viterbi. An intuitive justification and a simplified implementation of the map decoder for convolutional codes. *IEEE Journal on Selected Areas in Communications*, 16(2):260–264, 1998.

[97] Matthias Wildemeersch, Tony QS Quek, Marios Kountouris, Alberto Rabbachin, and Cornelis H Slump. Successive interference cancellation in heterogeneous networks. *IEEE transactions on communications*, 62(12):4440–4453, 2014.

[98] Jack H Winters. Optimum combining in digital mobile radio with cochannel interference. *IEEE Transactions on Vehicular Technology*, 33(3):144–155, 1984.

[99] Peter W Wolniansky, Gerard J Foschini, GD Golden, and Reinaldo A Valenzuela. V-BLAST: An architecture for realizing very high data rates over the rich-scattering wireless channel. In *Signals, Systems, and Electronics, 1998. ISSSE 98. 1998 URSI International Symposium on*, pages 295–300. IEEE, 1998.

[100] Shaoyi Xu, Yan Li, Yuan Gao, Yang Liu, and Haris Gačanin. Opportunistic coexistence of LTE and WiFi for future 5G system: experimental performance evaluation and analysis. *IEEE Access*, 6:8725–8741, 2018.

[101] Yubo Yan, Panlong Yang, Xiang-Yang Li, Yafei Zhang, Jianjiang Lu, Lizhao You, Jiliang Wang, Jinsong Han, and Yan Xiong. Wizbee: Wise Zigbee coexistence via interference cancellation with single antenna. *IEEE Transactions on Mobile Computing*, 14(12):2590–2603, 2015.

[102] Yan Yubo, Yang Panlong, Li Xiangyang, Tao Yue, Zhang Lan, and You Lizhao. Zimo: Building cross-technology mimo to harmonize zigbee smog with wifi flash without intervention. In *Proceedings of the 19th annual international conference on Mobile computing & networking*, pages 465–476. ACM, 2013.

[103] Sangki Yun and Lili Qiu. Supporting WiFi and LTE co-existence. In *Computer Communications (INFOCOM), 2015 IEEE Conference on*, pages 810–818. IEEE, 2015.

[104] Duzhong Zhang, Quan Liu, Lin Chen, and Wenjun Xu. Survey on coexistence of heterogeneous wireless networks in 2.4 ghz and tv white spaces. *International Journal of Distributed Sensor Networks*, 13(4):1550147717703966, 2017.

[105] Xu Zhang and Edward W Knightly. Watch: WiFi in active tv channels. *IEEE Transactions on Cognitive Communications and Networking*, 2(4):330–342, 2016.

[106] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo. Full duplex techniques for 5g networks: self-interference cancellation, protocol design, and relay selection. *IEEE Communications Magazine*, 53(5):128–137, May 2015.